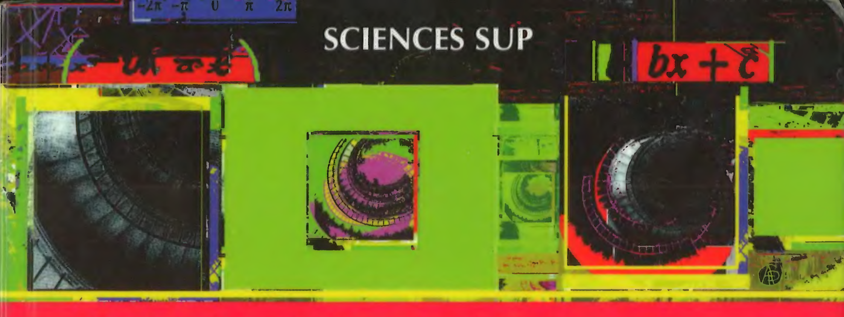


Cours et exercices corrigés

Licence • Master

LOGIQUE MATHÉMATIQUE

2. Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles

Préface de Jean-Louis Krivine

René Cori
Daniel Lascar



LOGIQUE MATHÉMATIQUE

2. Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles


http://www.dunod.com
SCIENCES ET TECHNIQUES
INFORMATIQUE Dunod & Microsoft Press
GESTION MANAGEMENT
SCIENCES HUMAINES
Acheter en ligne
Nouveautés
DUNOD
Microsoft Press
EdiScience ETSF
InterÉditions
Compléments en ligne
Magazine et interviews d'auteurs

LOGIQUE MATHÉMATIQUE

2. Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles

Cours et exercices corrigés

René Cori
Maître de conférences à l'université Paris 7 - Denis Diderot

Daniel Lascar
Directeur de recherches au CNRS

Préface de Jean-Louis Krivine

DUNOD

L'édition originale de cet ouvrage a été publiée en 1993 aux éditions Masson dans la collection *Axiomes*, coordonnée par J.-L. Krivine.

Illustration de couverture : *Lionel Auvergne*

ISBN 2 10 005453 8

PREFACE

La logique est, en France, une discipline traditionnellement négligée dans les études scientifiques universitaires. Cela tient, sans doute, à l'histoire récente des mathématiques dans notre pays, dominées pendant longtemps par l'école Bourbaki, dont, comme on sait, la logique n'était pas le fort. La logique part, en effet, d'une réflexion sur l'activité mathématique, et une réaction épidermique courante du mathématicien est de dire : « A quoi bon tout cela ? nous ne sommes pas des philosophes, et ce n'est pas en se cassant la tête sur le modus ponens ou le tiers exclu que l'on résoudra les grandes conjectures, ni même les petites ». Voire ...

Cependant un élément nouveau, et de taille, est venu clore ce débat un peu byzantin sur l'intérêt de la logique : l'explosion de l'informatique, dans tous les domaines de la vie économique et scientifique, dont l'onde de choc a fini par atteindre les mathématiciens eux-mêmes.

Et petit à petit, une évidence se fait jour : pour cette nouvelle science en train de naître, les bases théoriques ne sont autres que cette discipline si discutée : la logique mathématique.

Il est vrai que certains domaines de la logique ont été mis à contribution plus vite que d'autres. Le calcul booléen, bien sûr, pour la conception et l'étude des circuits ; la récursivité, qui est la théorie des fonctions calculables sur machine ; le théorème de Herbrand, la résolution et l'unification, qui sont à la base de la programmation dite « logique » (langage PROLOG) ; la théorie de la démonstration, et les divers avatars du théorème de complétude, qui se révèlent de puissants outils d'analyse pour les langages de programmation évolués ...

Mais, au train où vont les choses, on peut penser que le tour ne saurait tarder à venir, même pour des domaines restés encore complètement « purs », comme la théorie des ensembles, par exemple.

Comme il se doit, l'interaction n'est pas à sens unique, loin de là, et un afflux d'idées et d'intuitions nouvelles et profondes, issues de l'informatique, est venu renouveler tous ces secteurs de la logique. Cette discipline est maintenant l'une des plus vivantes qui soient en mathématiques, et en évolution très rapide.

Aussi l'utilité et l'actualité d'un ouvrage d'initiation générale en logique ne font-elles pas de doute, et ce livre vient donc à son heure. Issu d'un enseignement du D.E.A. de

Logique et fondements de l'Informatique à l'Université Paris 7, il couvre un vaste panorama : algèbre de Boole, récursivité, théorie des modèles, théorie des ensembles, modèles de l'arithmétique et théorèmes de Gödel.
La notion de modèle est un élément central de l'ouvrage, et c'est à fort juste titre, car elle a aussi une place centrale en logique : malgré (ou grâce à) son caractère simple et même élémentaire, elle en éclaire tous les domaines, y compris ceux qui en paraissent les plus éloignés. Comment comprendre, par exemple, une démonstration de consistance en théorie des ensembles, sans avoir d'abord maîtrisé le concept de modèle de cette théorie ? comment saisir vraiment le théorème de Gödel sans avoir une idée sur les modèles non standard de l'arithmétique de Peano ? L'acquisition de ces notions sémantiques est, je le crois, caractéristique d'une véritable formation de logicien, à quelque niveau que ce soit. R. Cori et D. Lascar le savent fort bien, et leur livre va tout à fait dans ce sens. Qui plus est, ils ont réussi le difficile pari d'allier toute la rigueur nécessaire avec la clarté, le souci pédagogique et l'agrément de la lecture.
Nous disposons donc là d'un outil remarquable pour l'enseignement de la logique mathématique, et, vu le développement de la demande en ce domaine, il devrait connaître un franc succès. C'est, bien sûr, tout ce que je lui souhaite.

Jean-Louis Krivine

TABLE DES MATIERES DU TOME I

TABLE DES MATIERES DU TOME II

CONTENTS

VOLUME I

VOLUME II

Ce livre est dédié
à l'éducation et à la géographie
physiques.

R.C. et D.L.

AVANT-PROPOS

Ce livre fait suite à une expérience de plusieurs années d'enseignement de la logique à l'U.F.R. de Mathématiques de l'Université Paris 7, tant en deuxième cycle que dans le D.E.A. de Logique et Fondements de l'Informatique.

Dès que nous avons commencé à préparer nos premiers cours, nous avons constaté qu'il allait être bien difficile d'indiquer à nos étudiants des ouvrages généraux de logique écrits (ou même traduits) en français. Nous avons alors décidé de profiter de l'occasion qui nous était donnée de remédier à cela. Les premières versions des huit chapitres qu'on va lire ont donc été rédigées en même temps que leur contenu était enseigné. Nous tenons à remercier chaleureusement tous les étudiants qui ont ainsi contribué à une amélioration sensible de l'exposé initial.

Nos remerciements vont aussi à tous nos collègues et amis logiciens, de Paris 7 ou d'ailleurs, qui nous ont apporté une aide très appréciée, par leurs nombreuses remarques et par un soutien moral d'une rare qualité. Presque tous sont co-auteurs de cet ouvrage, puisque, pour constituer les listes d'exercices qui accompagnent chaque chapitre, nous avons puisé sans retenue dans le fonds inestimable que représentent les centaines et centaines de textes qui ont été proposés aux étudiants, pendant plus de vingt-cinq années, au cours desquelles l'Université Paris 7, pionnière en la matière, a organisé des enseignements de logique ouverts à un large public.

Parvenu à ce stade, le lecteur s'attend en général à une phrase du type suivant : « ils sont tellement nombreux que nous ne pouvons évidemment pas les citer tous ». En effet, ils sont très nombreux, ceux à qui va notre gratitude, mais pourquoi ne pas essayer de les citer tous ?

Merci, donc, à Josette Adda, Marouan Ajlani, Daniel Andler, Gilles Amiot, Fred Appenzeller, Jean-Claude Archer, Jean-Pierre Azra, Jean-Pierre Bénéjam, Chantal Berline, Claude-Laurent Bernard, Georges Blanc, Elisabeth Bouscaren, Albert Burroni, Jean-Pierre Calais, Zoé Chatzidakis, Peter Clote, François Conduché, Jean Coret, Maryvonne Daguenet, Vincent Danos, Max Dickmann, Patrick Dehornoy, Françoise Delon, Florence Duchêne, Jean-Louis Duret, Marie-Christine Ferbus, Jean-Yves Girard, Danièle Gondard, Catherine Gourion, Serge Grigorieff, Ursula Gropp, Philippe Ithier, Bernard Jaulin, Ying Jiang, Thierry Joly, Anatole Khélif, Georg Kreisel, Jean-Louis Krivine, Ramez Labib-Sami, Daniel Lacombe, Thierry Lacoste, Richard Lassaigne, Yves

Legrand-Gérard, Alain Louveau, François Lucas, Kenneth Mac Aloon, Gilles Macario-Rat, Sophie Malecki, Jean Malifaud, Pascal Manoury, François Métayer, Marie-Hélène Mourgues, Catherine Muhlrad-Greif, Francis Oger, Michel Parigot, Donald Pelletier, Marie-Jeanne Perrin, Bruno Poizat, Jean Porte, Claude Précetti, Christophe Raffalli, Laurent Régnier, Jean-Pierre Ressayre, Philippe Royer, Paul Rozière, Gabriel Sabbagh, Claire Santoni, Marianne Simonot, Gerald Stahl, Jacques Stern, Anne Strauss, Jacques Van de Wiele, Françoise Ville.

Nous tenons aussi à rendre hommage au travail administratif et technique remarquable accompli par Mesdames Sylviane Barrier, Gisèle Goémine et Claude Orieux.

Que ceux que nous avons oubliés nous pardonnent. Ils sont tellement nombreux que nous ne pouvons les citer tous.

MODE D'EMPLOI

Le livre est organisé en deux tomes. Le premier comporte les chapitres 1 à 4, le second les chapitre 5 à 8. Les notions exposées dans un chapitre donné supposent connues celles qui ont fait l'objet des chapitres antérieurs (mais les chapitres 2 et 5 font exception à cette règle).

Chacun des huit chapitres est divisé en sections, elles-mêmes composées d'un certain nombre de sous-sections, numérotées de la façon la plus simple qui soit : 2.3 annonce le début de la troisième sous-section de la section 2. Les définitions, lemmes, propositions, théorèmes, corollaires et remarques sont identifiés par la sous-section dans laquelle ils figurent ; lorsqu'il y a, par exemple, deux lemmes dans une même sous-section, ils sont numérotés : lemme 1 et lemme 2. Cela conduit à un système de références internes tout à fait explicite qu'il est inutile de détailler davantage. Précisons simplement que les références internes à un chapitre ne comportent pas l'indication de celui-ci.

Les sections sont, en général, divisées par des intertitres qui concernent plusieurs sous-sections. Ces intertitres se retrouvent dans la table des matières mais ne font pas partie du système de références.

Le début et la fin des démonstrations sont respectivement signalés par les signes ☹ et ☺.

A la fin de chaque chapitre figure une liste d'énoncés d'exercices. Les solutions sont regroupées à la fin du tome correspondant. Dans les solutions d'exercices, les références sont traitées comme dans le chapitre correspondant : celles qui ne comportent pas d'indication de chapitre sont internes ; ainsi, la mention « découle du corollaire 2.4 » que l'on trouve dans le corrigé de l'exercice 21 du chapitre 5 se rapporte au corollaire 2.4 du chapitre 5. Les solutions sont, surtout pour les premiers chapitres, assez détaillées.

Notre lecteur est supposé avoir une certaine pratique des mathématiques, et des connaissances correspondant, grosso modo, aux mathématiques classiques enseignées dans les lycées et dans les premiers cycles universitaires. Nous nous référerons librement à ce que nous avons appelé ce « fonds commun », en particulier dans les exemples et les exercices.

Cependant, le cours lui-même ne suppose dans l'ensemble aucune connaissance particulière préalable.

Nous utilisons la terminologie et les notations les plus répandues pour tout ce qui relève du (méta-)langage mathématique ensembliste habituel : opérations sur les ensembles, relations, applications, etc, de même que pour les ensembles les plus fréquentés en mathématiques : $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

Si E et F sont des ensembles, et si f est une application définie sur une partie de E et à valeurs dans F, le **domaine** de f est noté dom(f) (c'est l'ensemble des éléments de E en lesquels f est définie), et son **image** est notée Im(f) (c'est l'ensemble des éléments y appartenant à F tels que, pour au moins un élément x de E, on ait $y = f(x)$). Si A est une partie du domaine de f, la **restriction** de f à A est l'application de A dans F, notée $f\restriction_A$, qui, à chaque élément x de A, associe f(x). L'image de l'application $f\restriction_A$ est aussi appelée **image directe de A par f** et notée f[A]. Si B est une partie de F, l'**image réciproque de B par f** est la partie de E, notée $f^{-1}[B]$, constituée des éléments x de E tels que $f(x) \in B$. En fait, étant donnée une application f d'un ensemble E dans un ensemble F, on peut lui associer canoniquement une application de $\mathfrak{P}(E)$ (ensemble des parties de E) dans $\mathfrak{P}(F)$: l'application « image directe », notée $\bar{f}$, qui, à toute partie A de E, associe f[A], qu'on pourra donc également noter $\bar{f}(A)$. On peut de même associer à f une application de $\mathfrak{P}(F)$ dans $\mathfrak{P}(E)$, l'application « image réciproque » , notée $\bar{f}^{-1}$, qui, à toute partie B de F, associe $f^{-1}[B]$, qu'on notera donc aussi $\bar{f}^{-1}(B)$. (Voir aussi l'exercice 19 du chapitre 2.)

Il est peut-être également utile de donner quelques précisions sur la notion de mot sur un alphabet, qui sera la première utilisée :

Soit E un ensemble, fini ou infini, que nous appelons **alphabet**. Un **mot** m sur l'alphabet E est une suite finie d'éléments de E (c'est-à-dire une application de l'ensemble $\{0,1,...,n-1\}$ (n étant un entier) dans E) ; on écrira $m = (a_0,a_1,...,a_{n-1})$ ou même $a_0a_1...a_{n-1}$ le mot qui est l'application de domaine $\{0,1,...,n-1\}$ qui à i $(0 \leqslant i \leqslant n-1)$ fait correspondre a_i. L'entier n est appelé la **longueur** du mot m et est notée lg[m]. L'ensemble des mots sur E est noté $\mathcal{M}(E)$.

Si $n = 0$, on obtient le **mot vide**. On fera l'abus de langage consistant à identifier un mot (a) de longueur 1 avec l'élément a. L'ensemble $\mathcal{M}(E)$ peut être muni d'une opération binaire, la **concaténation** : soient $m_1 = (a_0,a_1,...,a_{n-1})$ et $m_2 = (b_0,b_1,...,b_{m-1})$ deux mots. On peut former le nouveau mot $m = (a_0,a_1,...,a_{n-1},b_0,b_1,...,b_{m-1})$ (c'est-à-dire l'application m de $\{0,1,...,n+m-1\}$ définie comme suit : si $0 \leqslant i \leqslant n-1$, alors $m(i) = a_i$; si $n \leqslant i \leqslant n+m-1$, alors $m(i) = b_{i-n}$). Ce mot est appelé le **concaténé de m_1 avec m_2** et est noté m_1m_2. Cette notation est justifiée par le fait que la concaténation est une opération associative.

Etant donnés deux mots m et m_1, on dit que m_1 est un **segment initial de** m s'il existe un mot m_2 tel que $m = m_1m_2$. Autrement dit, si $m = (a_0,a_1,...,a_{n-1})$, les segments initiaux de m sont les mots de la forme $(a_0,a_1,...,a_{p-1})$ où p est un entier inférieur ou égal à n. On dit que m_1 est un **segment final de** m s'il existe un mot m_2 tel que $m = m_2m_1$; les segments finaux de $(a_0,a_1,...,a_{n-1})$ sont donc les mots de la forme $(a_p,a_{p+1},..., a_{n-1})$ (p

étant un entier inférieur ou égal à n). En particulier, le mot vide et m lui-même sont des segments initiaux et des segments finaux de m. Un segment (initial ou final) de m est **propre** s'il est différent de m et du mot vide.

Lorsqu'un élément b de l'alphabet « apparaît » dans un mot $m = a_0a_1...a_{n-1}$, on dit qu'il **a une occurrence dans** m, et les divers « endroits » où il apparaît s'appellent les **occurrences de** b **dans** m. On peut naturellement être plus précis et plus formel : on dira que b **a une occurrence dans** m si b est égal à l'un des a_i, pour i compris entre 0 et $n-1$ (c'est-à-dire si b appartient à l'image de m) ; une **occurrence de** b **dans** m est un entier k, inférieur ou égal à $\lg[m]$, tel que $b = a_k$. Par exemple, la troisième occurrence de b dans m est le troisième élément de l'ensemble $\{k ; 0 \leqslant k \leqslant n-1 \text{ et } a_k = b\}$ rangé dans l'ordre croissant. Ce formalisme ne sera pas explicitement utilisé dans le cours : l'idée donnée au début de ce paragraphe sera amplement suffisante pour ce que nous aurons à faire.

Les faits suivants sont à peu près évidents et seront constamment utilisés :

- pour tous mots m_1 et m_2, $\lg[m_1m_2] = \lg[m_1] + \lg[m_2]$;
- pour tous mots m_1, m_2 et m_3, l'égalité $m_1m_2 = m_1m_3$ implique l'égalité $m_2 = m_3$ (on dit que l'on peut **simplifier à gauche**) ;
- pour tous mots m_1, m_2 et m_3, l'égalité $m_1m_2 = m_3m_2$ implique l'égalité $m_1 = m_3$ (on peut **simplifier à droite**) ;
- pour tous mots m_1, m_2, m_3 et m_4, si $m_1m_2 = m_3m_4$, alors m_1 est un segment initial de m_3 ou m_3 est un segment initial de m_1. D'une façon analogue, avec les mêmes hypothèses, m_2 est un segment final de m_4 ou m_4 est un segment final de m_2 ;
- si m_1 est un segment initial de m_2 et m_2 est un segment initial de m_1, alors $m_1 = m_2$.

On utilisera aussi le fait que $\mathscr{M}(E)$ est dénombrable si E est fini ou dénombrable (c'est le théorème 4.9 du chapitre 7).

Chapitre 5

Récursivité

Les fonctions récursives sont des fonctions de $\mathbb{N}^p$ *(une puissance cartésienne de l'ensemble des entiers naturels) dans* $\mathbb{N}$. *Intuitivement, ce sont les fonctions qui sont effectivement calculables, ou, si l'on préfère, pour lesquelles il existe un algorithme de calcul, ou encore qui peuvent être calculées par une machine. Il faut noter que c'est seulement la possibilité théorique d'un calcul mécanique qui est considérée ici, le calcul d'une fonction pouvant très bien prendre un temps beaucoup trop long pour que l'on puisse raisonnablement l'envisager.*

Dans une première section, on définit une classe de fonctions, les fonctions récursives primitives, qui répondent manifestement au critère du paragraphe précédent. On essaiera de convaincre le lecteur que cette classe est déjà fort riche en montrant que toutes les fonctions qui viennent à l'esprit sont récursives primitives. Malheureusement, les fonctions récursives primitives n'épuisent pas la classe que nous voulons décrire : dans la seconde section, on construira une fonction, la fonction d'Ackermann, qui n'est pas récursive primitive bien qu'elle soit effectivement calculable. On définit donc une classe plus riche, la classe des fonctions récursives. Mais en fait, il est nécessaire, pour des raisons qui apparaîtront aussi à la quatrième section, de définir une classe plus compliquée et a priori moins naturelle, la classe des fonctions partielles récursives. Une fonction partielle f *à* p *variables est une application d'un sous-ensemble* E *de* $\mathbb{N}^p$ *dans* $\mathbb{N}$ *et elle est récursive s'il existe un algorithme qui la calcule dans le sens suivant : si on applique l'algorithme pour calculer* $f(n_1,n_2,\ldots,n_p)$ *et si* $(n_1,n_2,\ldots,n_p) \in E$, *alors il effectuera le calcul ; si* $(n_1,n_2,\ldots,n_p) \notin E$, *alors l'algorithme ne s'arrêtera jamais. Il semble bien que l'on ait cerné la notion de fonction calculable : on n'a jamais pu trouver de fonction que l'on sache effectivement calculer et dont on ne sache démontrer qu'elle est récursive ou partielle récursive.*

Les machines de Turing, qui sont une version mathématique des machines à calculer ou des ordinateurs, sont définies dans la troisième section. On montre que les fonctions qu'elles calculent sont exactement les fonctions partielles récursives. Il y a bien d'autres machines mathématiques qui ont été définies, mais nous avons préféré les machines de Turing, car leur intérêt est multiple : premièrement historique, car ce sont les premiers modèles de machines mathématiques qui aient été introduits ; ensuite pédagogique, car on voit comment la machine fonctionne de façon quasiment mécanique ; enfin théorique, car elles permettent de montrer les importants théorèmes d'énumération et du point fixe. Ceci sera fait dans la quatrième section.

1. FONCTIONS ET ENSEMBLES RECURSIFS PRIMITIFS

Les premières définitions

1.1 On va définir l'ensemble des fonctions récursives primitives par induction, par un procédé analogue à celui que nous avons utilisé pour définir les formules du calcul propositionnel ou du calcul des prédicats : ce sera la plus petite classe de fonctions contenant certaines fonctions que l'on va spécifier et close pour certaines opérations. On a besoin de quelques justifications et notations avant de donner la définition.

• Soit p un entier ; on désignera par $\mathfrak{F}_p$ l'ensemble des applications de $\mathbb{N}^p$ dans $\mathbb{N}$. On conviendra que, si $p = 0$, $\mathbb{N}^p$ ne contient que la suite vide et les éléments de $\mathfrak{F}_0$ peuvent alors être identifiés avec les éléments de $\mathbb{N}$; on notera $\mathfrak{F}$ l'ensemble $\bigcup_{p\in\mathbb{N}} \mathfrak{F}_p$.

• Si i est un entier compris entre 1 et p, la **i-ème projection** P_p^i est la fonction de $\mathfrak{F}_p$ définie par :

$$P_p^i(x_1,x_2,\ldots,x_p) = x_i.$$

• On utilisera dans ce chapitre les notations suivantes, provenant du lambda-calcul : avec ces notations, la fonction P_p^i s'écrit :

$$P_p^i = \lambda x_1x_2\ldots x_p.x_i.$$

D'une façon générale, $\lambda x_1x_2\ldots x_p.t$, où t est une expression faisant intervenir les variables $x_1,x_2,\ldots x_p$, désigne la fonction qui à $n_1,n_2,\ldots,n_p$ fait correspondre $t(n_1,n_2,\ldots,n_p)$. Cette notation peut aussi être utilisée pour des fonctions de $\mathbb{N}^p$ dans $\mathbb{N}^q$: par exemple $\lambda xy.(x + y,3x + 2y)$ est la fonction de $\mathbb{N}^2$ dans lui-même qui au couple (m,n) fait correspondre le couple $(m + n,3m + 2n)$.

• Par définition, **la fonction successeur** S est la fonction $\lambda x.x+1$, c'est-à-dire la fonction de $\mathfrak{F}_1$ qui à chaque entier n fait correspondre $n+1$.

• Si $f_1, f_2,\ldots,f_n$ appartiennent à $\mathfrak{F}_p$ et g appartient à $\mathfrak{F}_n$, **la fonction composée** $h = g(f_1,f_2,\ldots,f_n)$ est l'élément de $\mathfrak{F}_p$ égal à

$$\lambda x_1x_2\ldots x_p.g(f_1(x_1,x_2,\ldots,x_p),f_2(x_1,x_2,\ldots,x_p),\ldots,f_n(x_1,x_2,\ldots,x_p)).$$

1.2 **Définition par récurrence** : C'est un procédé de définition de fonctions qui est justifié par le fait évident suivant : soient $g \in \mathfrak{F}_p$ et $h \in \mathfrak{F}_{p+2}$; alors il y a une et une seule fonction $f \in \mathfrak{F}_{p+1}$ qui, pour tous $x_1,x_2,\ldots,x_p$ et y de $\mathbb{N}$, vérifie les conditions suivantes :

i) $f(x_1,x_2,\ldots,x_p,0) = g(x_1,x_2,\ldots,x_p)$;

ii) $f(x_1,x_2,\ldots,x_p,y+1) = h(x_1,x_2,\ldots,x_p,y,f(x_1,x_2,\ldots,x_p,y))$.

On dit que f est **la fonction définie par récurrence** à partir de g (**condition initiale**) et h (**étape de récurrence**).

REMARQUE : il faut se convaincre que la définition par récurrence permet le calcul effectif de la fonction définie. Plus précisément, supposons que g et h sont deux fonctions comme ci-dessus et que, de plus, on sache les calculer effectivement à l'aide d'algorithmes $\mathcal{A}_1$ et $\mathcal{A}_2$ respectivement. Alors, il n'est pas difficile d'imaginer un autre algorithme qui calcule la fonction f définie par récurrence à partir de g et h : pour calculer $f(n_1,n_2,\ldots,n_p,m)$, il faut d'abord calculer $f(n_1,n_2,\ldots,n_p,0)$ (qui est égal à $g(n_1,n_2,\ldots,n_p)$; on utilise l'algorithme $\mathcal{A}_1$), puis $f(n_1,n_2,\ldots,n_p,1)$ (en utilisant la définition de f et l'algorithme $\mathcal{A}_2$) et on continue jusqu'à obtenir la valeur voulue.

1.3 DEFINITION : *L'ensemble des **fonctions récursives primitives** est le plus petit des sous-ensembles* E *de* $\mathfrak{F}$ *satisfaisant les conditions suivantes :*

i) E *contient toutes les fonctions constantes de* $\mathbb{N}^p$ *dans* $\mathbb{N}$ *pour tout entier* p.

ii) E *contient toutes les projections* P_p^i *pour tous entiers* p *et* i *tels que* $1 \leqslant i \leqslant p$.

iii) E *contient la fonction successeur* S.

iv) E *est clos par composition, ce qui veut dire que, si* n *et* p *sont des entiers, si* $f_1,f_2,\ldots,f_n$ *sont des fonctions de* $\mathfrak{F}_p$ *qui appartiennent à* E, *et si* $g \in \mathfrak{F}_n$ *est aussi dans* E, *alors la fonction composée* $g(f_1,f_2,\ldots,f_n)$ *appartient à* E.

v) E *est clos par récurrence, ce qui veut dire que, si* p *est un entier, si* g *appartenant à* $\mathfrak{F}_p$ *et* h *appartenant à* $\mathfrak{F}_{p+2}$ *sont toutes les deux dans* E, *alors la fonction* f *définie par récurrence à partir de* g *et* h *est aussi dans* E.

REMARQUE : Comme on l'a fait pour l'ensemble des formules du calcul propositionnel ou du calcul des prédicats, on aurait pu donner une définition « par le bas » de l'ensemble des fonctions récursives primitives. On pose :

$R_0 = \{ \gamma \ ; p \in \mathbb{N}$ et γ est une fonction constante de $\mathbb{N}^p$ dans $\mathbb{N} \} \cup \{ P_p^i \ ; 1 \leqslant i \leqslant p \} \cup \{ S \}$,

et, pour tout entier n :

$R_{n+1} = R_n \cup \{ h$; h est obtenue par récurrence à partir de deux fonctions de $R_n \}$

$\cup \{ h$; h est obtenue par composition à partir de fonctions de $R_n \}$;

alors l'ensemble des fonctions récursives primitives est égal à $\bigcup_{n \in \mathbb{N}} R_n$.

Pour montrer qu'une fonction est récursive primitive, il faut montrer comment l'obtenir, à l'aide des clauses *iv)* et *v)* et à partir des fonctions décrites en *i)*, *ii)*, *iii)*, ou plus généralement à partir de fonctions dont on sait déjà qu'elles sont récursives primitives. On verra des exemples très bientôt.

D'autre part, pour montrer que toutes les fonctions récursives primitives possèdent une certaine propriété $\mathcal{P}$, il suffit de montrer que les fonctions mentionnées aux alinéas *i)*, *ii)* et *iii)* ont cette propriété et que la classe des fonctions satisfaisant $\mathcal{P}$ est close par composition et par récurrence.

On peut voir aussi que, pour toute fonction f récursive primitive, il existe un algorithme la calculant : c'est vrai pour les fonctions de R_0 et, si c'est vrai pour les fonctions de R_n, ça l'est aussi pour celles de R_{n+1}.

1.4 DEFINITION : *On dit qu'un ensemble* $A \subseteq \mathbb{N}^p$ *est* ***récursif primitif*** *si sa fonction caractéristique est récursive primitive.*

Rappelons que la **fonction caractéristique** χ_A de l'ensemble A est définie par :

$\chi_A(n_1,n_2,...,n_p)=1$ si $(n_1,n_2,...,n_p) \in A$;

$\chi_A(n_1,n_2,...,n_p)=0$ sinon.

La fonction caractéristique de l'ensemble A sera notée χ_A ou $\chi(A)$ suivant les exigences de la typographie. Si $\mathcal{P}(x_1,x_2,...,x_p)$ est une propriété portant sur les entiers $x_1,x_2,...,x_p$ (on parlera aussi de prédicat d'arité p), on dira que $\mathcal{P}$ est récursive primitive si l'ensemble

$$\{(x_1,x_2,...,x_p) \ ; (x_1,x_2,...,x_p) \text{ vérifie } \mathcal{P}\}$$

est récursif primitif.

Exemples et propriétés de clôture

1.5 • L'addition $\lambda xy.x + y$ est récursive primitive : en effet, elle peut se définir par récurrence par :

$x + 0 = x$;

$x + (y + 1) = (x + y) + 1$.

Soyons pour cet exemple (mais pour celui-ci seulement) d'une précision maniaque. Notons ad la fonction addition ($ad = \lambda xy.x + y$). Alors

$ad(x,0)=P_1^1(x)$;

$ad(x,y + 1) = S(P_3^3(x,y,ad(x,y)))$.

• La multiplication est aussi récursive primitive. On peut la définir par récurrence à partir de l'addition :

$x \cdot 0 = 0$;

$x \cdot (y+1) = x \cdot y + x$.

• La fonction $\lambda xy.x^y$ est aussi récursive primitive. Elle peut se définir par :

$x^0 = 1$;

$x^{y+1} = x^y \cdot x$.

• Convenons de noter $x \dot{-} 1$ l'entier égal à $x - 1$ si $x > 0$ et à 0 sinon. Alors la fonction $\lambda x.x \dot{-} 1$ est récursive primitive. En effet elle peut être définie par récurrence par :

$0 \dot{-} 1 = 0$;

$(x+1) \dot{-} 1 = x$.

• Plus généralement, notons $x \dot{-} y$ l'entier égal à $x - y$ si $x \geqslant y$ et à 0 sinon. La fonction $\lambda xy.x \dot{-} y$ est elle aussi récursive primitive :

$x \dot{-} 0 = x$;

$x \dot{-} (y+1) = (x \dot{-} y) \dot{-} 1$.

• Définissons la fonction sg par : $sg(0) = 0$ et $sg(x) = 1$ si $x \neq 0$. La fonction sg est récursive primitive : en effet $sg(x) = 1 \dot{-} (1 \dot{-} x)$.

• Le prédicat $x > y$ est récursif primitif (ce qui veut dire que l'ensemble $\{(x,y) ; x > y\}$ est récursif primitif). En effet, la fonction caractéristique de cet ensemble est égale à $sg(x \dot{-} y)$. De même le prédicat $x \geqslant y$, dont la fonction caractéristique est $sg((x+1) \dot{-} y)$, est récursif primitif.

1.6 Nous allons maintenant montrer que les fonctions récursives primitives et les prédicats récursifs primitifs jouissent d'un certain nombre de propriétés de clôture.

• L'ensemble des fonctions récursives primitives est clos par substitution de variables : si $f \in \mathfrak{F}_p$ est récursive primitive et si σ est une application de l'ensemble $\{1,2,\ldots,p\}$ dans lui-même, alors la fonction $\lambda x_1x_2\ldots x_p.f(x_{\sigma(1)},x_{\sigma(2)},\ldots,x_{\sigma(p)})$ est aussi récursive primitive. En effet, cette fonction est égale à $f(P_p^{\sigma(1)},P_p^{\sigma(2)},\ldots,P_p^{\sigma(p)})$.

• Si $A \subseteq \mathbb{N}^n$ est récursif primitif et si $f_1,f_2,\ldots,f_n$ appartiennent à $\mathfrak{F}_p$ et sont récursives primitives, alors l'ensemble

$$\{(x_1,x_2,\ldots,x_p) \ ; (f_1(x_1,x_2,\ldots,x_p),f_2(x_1,x_2,\ldots,x_p),\ldots,f_n(x_1,x_2,\ldots,x_p)) \in A\}$$

est aussi récursif primitif (sa fonction caractéristique est $\chi_A(f_1,f_2,\ldots,f_n)$).

• On déduit facilement de ce qui précède que, si f et g sont deux fonctions récursives primitives de $\mathfrak{F}_p$, alors les ensembles

$\{(x_1,x_2,\ldots,x_p) \ ; f(x_1,x_2,\ldots,x_p) > g(x_1,x_2,\ldots,x_p)\}$,

$\{(x_1,x_2,\ldots,x_p) \ ; f(x_1,x_2,\ldots,x_p) = g(x_1,x_2,\ldots,x_p)\}$

et $\{(x_1,x_2,\ldots,x_p) \ ; f(x_1,x_2,\ldots,x_p) < g(x_1,x_2,\ldots,x_p)\}$

sont récursifs primitifs. En particulier, l'ensemble $\{(x_1,x_2,\ldots,x_p) \ ; f(x_1,x_2,\ldots,x_p) > 0\}$ est récursif primitif.

• Pour chaque entier p, l'ensemble des sous-ensembles récursifs primitifs de $\mathbb{N}^p$ est clos pour les opérations booléennes : si A et B sont des sous-ensembles récursifs primitifs de $\mathbb{N}^p$, il en est de même de $A \cap B$, $A \cup B$ et $\mathbb{N}^p - A$. On peut en effet calculer les fonctions caractéristiques de ces nouveaux ensembles :

$$\chi(A \cap B) = \chi(A).\chi(B) ;$$
$$\chi(A \cup B) = sg(\chi(A) + \chi(B)) ;$$
$$\chi(\mathbb{N}^p - A) = 1 \dot{-} \chi(A).$$

Remarquons en particulier que $A - B = A \cap (\mathbb{N}^p - B)$ est récursif primitif.

1.7 • **Schéma de définition par cas** : soient f et g deux fonctions récursives primitives de $\mathfrak{F}_p$ et A un sous-ensemble récursif primitif de $\mathbb{N}^p$; alors la fonction h définie par :

$$h(x_1,x_2,...,x_p) = f(x_1,x_2,...,x_p) \text{ si } (x_1,x_2,...,x_p) \in A ,$$
$$h(x_1,x_2,...,x_p) = g(x_1,x_2,...,x_p) \text{ sinon,}$$

est récursive primitive. Il suffit de remarquer que $h = f.\chi(A) + g.\chi(\mathbb{N}^p \dot{-} A)$.

On peut généraliser cette possibilité de définition par cas : soient $f_1,f_2,...,f_{n+1} \in \mathfrak{F}_p$ des fonctions récursives primitives et $A_1,A_2,...,A_n \subseteq \mathbb{N}^p$ des ensembles récursifs primitifs ; alors la fonction g définie par :

$g(x_1,x_2,...,x_p) = f_1(x_1,x_2,...,x_p)$ si $(x_1,x_2,...,x_p) \in A_1$,
$g(x_1,x_2,...,x_p) = f_2(x_1,x_2,...,x_p)$ si $(x_1,x_2,...,x_p) \notin A_1$ et $(x_1,x_2,...,x_p) \in A_2$,
$g(x_1,x_2,...,x_p) = f_3(x_1,x_2,...,x_p)$ si $(x_1,x_2,...,x_p) \notin A_1 \cup A_2$ et $(x_1,x_2,...,x_p) \in A_3$,
...
$g(x_1,x_2,...,x_p) = f_n(x_1,x_2,...,x_p)$ si $(x_1,x_2,...,x_p) \notin A_1 \cup A_2 \cup ... \cup A_{n-1}$ et $(x_1,x_2,...,x_p) \in A_n$,
$g(x_1,x_2,...,x_p) = f_{n+1}(x_1,x_2,...,x_p)$ si $(x_1,x_2,...,x_p) \notin A_1 \cup A_2 \cup ... \cup A_n$,

est une fonction récursive primitive. En effet, on peut remarquer que :

$$g = f_1 \cdot \chi(A_1) + f_2 \cdot \chi(A_2 - A_1) + f_3 \cdot \chi(A_3 - (A_1 \cup A_2)) + \cdots$$
$$+ f_n \cdot \chi(A_n - (A_1 \cup A_2 \cup ... \cup A_{n-1})) + f_{n+1} \cdot \chi(\mathbb{N}^p - (A_1 \cup A_2 \cup ... \cup A_n)).$$

• En corollaire, on voit que les fonctions $\lambda x_1x_2...x_p.sup(x_1,x_2,...,x_p)$ et $\lambda x_1x_2...x_p.inf(x_1,x_2,...,x_p)$ sont récursives primitives. Par exemple, $sup(x_1,x_2,...,x_p)$ peut être définie de la façon suivante :

$$sup(x_1,x_2,...,x_p) = x_1 \text{ si } x_1 \geqslant x_2 \text{ et } x_1 \geqslant x_3 \text{ et ... et } x_1 \geqslant x_p ;$$
$$sup(x_1,x_2,...,x_p) = x_2 \text{ sinon et si } x_2 \geqslant x_3 \text{ et ... et } x_2 \geqslant x_p, \text{ etc.}$$

1.8 • **Somme et produit limités** : soit f une fonction récursive primitive de $\mathfrak{F}_{p+1}$. Alors les fonctions

$$g = \lambda x_1x_2...x_py.\Sigma_{t=0}^{t=y} f(x_1,x_2,...,x_p,t)$$

et

$$h = \lambda x_1x_2...x_py.\prod_{t=0}^{t=y} f(x_1,x_2,...,x_p,t)$$

sont aussi récursives primitives. Elles se définissent facilement par récurrence. Pour la somme, par exemple :

$g(x_1,x_2,\ldots,x_p,0) = f(x_1,x_2,\ldots,x_p,0)$;

$g(x_1,x_2,\ldots,x_p,y+1) = g(x_1,x_2,\ldots,x_p,y) + f(x_1,x_2,\ldots,x_p,y+1)$.

En particulier, la fonction factorielle $\lambda x.x!$, qui peut être définie comme produit limité, est récursive primitive.

1.9 • **Schéma μ borné** : soit A un sous-ensemble récursif primitif de $\mathbb{N}^{p+1}$. Alors la fonction f de $\mathfrak{F}_{p+1}$ définie comme suit est récursive primitive :

$f(x_1,x_2,\ldots,x_p,z) = 0$ s'il n'existe pas d'entier $t \leqslant z$ tel que $(x_1,x_2,\ldots,x_p,t) \in A$;

sinon $f(x_1,x_2,\ldots,x_p,z)$ est égal au plus petit des entiers $t \leqslant z$ tels que $(x_1,x_2,\ldots,x_p,t) \in A$.

La fonction f est définie par récurrence, schéma de définition par cas et somme limitée :

$f(x_1,x_2,\ldots,x_p,0) = 0$;

$f(x_1,x_2,\ldots,x_p,z+1) = f(x_1,x_2,\ldots,x_p,z)$ si $\Sigma_{y=0}^{y=z}\chi_A(x_1,x_2,\ldots,x_p,y) \geqslant 1$;

$f(x_1,x_2,\ldots,x_p,z+1) = z+1$ sinon et si $(x_1,x_2,\ldots,x_p,z+1) \in A$;

$f(x_1,x_2,\ldots,x_p,z+1) = 0$ dans les autres cas.

Pour désigner cette fonction on utilisera la notation suivante :

$$f(x_1,x_2,\ldots,x_p,z) = \mu t \leqslant z\ ((x_1,x_2,\ldots,x_p,t) \in A).$$

(lire : « $f(x_1,x_2,\ldots,x_p,z)$ est le plus petit des entiers t inférieurs ou égaux à z tels que $(x_1,x_2,\ldots,x_p,t) \in A$ ».)

Dans l'utilisation de ce schéma, la condition $(x_1,x_2,\ldots,x_p,t) \in A$ aura souvent la forme « $g(x_1,x_2,\ldots,x_p,t) = 0$ », où g est une fonction récursive primitive.

• L'ensemble des prédicats récursifs primitifs est clos par **quantification bornée**. Cela veut dire que, si $A \subseteq \mathbb{N}^{p+1}$ est récursif primitif, il en est de même des ensembles :

$B = \{ (x_1,x_2,\ldots,x_p,z) \ ; \ \exists t \leqslant z\ (x_1,x_2,\ldots,x_p,t) \in A \}$

et $C = \{ (x_1,x_2,\ldots,x_p,z) \ ; \ \forall t \leqslant z\ (x_1,x_2,\ldots,x_p,t) \in A \}$.

En effet la fonction caractéristique de B est donnée par la formule :

$$\chi_B(x_1,x_2,\ldots,x_p,z) = sg(\Sigma_{t=0}^{t=z}\chi_A(x_1,x_2,\ldots,x_p,t),$$

et celle de C par :

$$\chi_C(x_1,x_2,\ldots,x_p,z) = \prod_{t=0}^{t=z}\chi_A(x_1,x_2,\ldots,x_p,t).$$

1.10 Profitons de ces connaissances toutes neuves pour montrer qu'un certain nombre de fonctions et d'ensembles sont récursifs primitifs :

• $\mathbb{N}$ est récursif primitif : sa fonction caractéristique est la fonction constante de $\mathfrak{F}_1$ égale à 1 ;

• l'ensemble des nombres pairs est aussi récursif primitif : sa fonction caractéristique χ est définie par récurrence par : $\chi(0) = 1$ et $\chi(n+1) = 1 \dot{-} \chi(n)$;

• la fonction $q(x,y)$ qui est égale à la partie entière de x/y si y n'est pas nul et à 0 si y est nul, est récursive primitive ; elle est définie par :

$$q(x,y) = \mu t \leqslant x\ ((t+1).y > x)\ ;$$

• l'ensemble $\{(x,y)\ ;\ y \text{ divise } x\}$ est récursif primitif : sa fonction caractéristique est égale à $1 \dot{-} sg(x \dot{-} y.q(x,y))$;

• l'ensemble $\{x\ ;\ x \text{ est un nombre premier}\}$ est récursif primitif : en effet x est premier si est seulement si $x > 1$ et $\forall y \leqslant x(y \leqslant 1$ ou $y = x$ ou y ne divise pas $x)$;

• la fonction π qui à l'entier n fait correspondre le $(n+1)$-ème nombre premier est récursive primitive : elle est définie par récurrence, grâce au schéma μ borné, de la façon suivante :

$$\pi(0) = 2\ ;$$
$$\pi(n+1) = \mu z \leqslant (\pi(n)! + 1)(z > \pi(n) \text{ et } z \text{ est premier}).$$

(On utilise ici le fait bien connu qu'il y a toujours un nombre premier strictement compris entre p et $p! + 2$.)

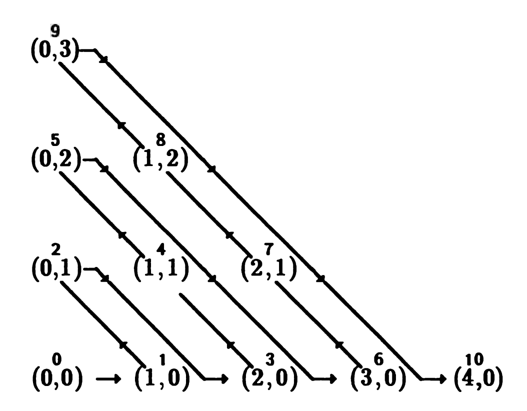
• On trouvera dans les exercices d'autres exemples de fonctions et d'ensembles récursifs primitifs.

Codages des suites

1.11 La notion de calculabilité ne s'applique pas seulement aux fonctions d'entiers dans les entiers. La généralisation la plus simple et la plus utile consiste à considérer des fonctions qui, à chaque suite finie d'entiers, font correspondre un entier ou même une autre suite finie. Pour pouvoir utiliser la théorie des fonctions récursives dans ce contexte, on va coder les suites finies d'entiers. Ce que l'on va faire exactement, c'est établir une application de l'ensemble des suites finies d'entiers à valeurs dans les entiers. Il faut évidemment que le codage que l'on utilise soit effectif, c'est-à-dire que l'on sache calculer l'entier correspondant à une suite donnée, et que, inversement, on puisse retrouver une suite à partir de son code. Il y a bien des façons de faire cela. On va donner ici deux codages dont on se servira par la suite.

PROPOSITION : *Pour chaque entier non nul* p, *il existe des fonctions récursives primitives* $\alpha_p \in \mathfrak{F}_p$, $\beta_p^1, \beta_p^2, \ldots, \beta_p^p \in \mathfrak{F}_1$ *qui possèdent la propriété suivante :* α_p *est une bijection de* $\mathbb{N}^p$ *sur* $\mathbb{N}$ *dont l'application réciproque est* $\lambda x.(\beta_p^1(x), \beta_p^2(x), \ldots, \beta_p^p(x))$.

☺ On va commencer par construire α_2. Pour cela, on numérote les couples d'entiers en suivant le schéma ci-dessous :



Plus précisément, on énumère les couples (x,y) en suivant les diagonales $x + y =$ constante. On commence par la diagonale $x + y = 0$ (qui ne contient qu'un seul couple), puis on passe à la diagonale $x + y = 1$ en commençant par le bas, etc. La valeur de $\alpha_2(x,y)$ est exactement le nombre de couples précédant (x,y) dans cette énumération. La diagonale $x + y = n$ a exactement $n + 1$ éléments. Donc avant le couple $(p + n,0)$ il y a $1 + 2 + \cdots + (n + p) = \frac{1}{2}(n + p)(n + p + 1)$ éléments. Le couple (p,n) se trouve sur la même diagonale que $(p + n,0)$ et exactement n places après lui. Par conséquent :

$$\alpha_2(p,n) = \tfrac{1}{2}(n + p + 1)(n + p) + n.$$

On remarque que α_2 est bien récursive primitive et supérieure ou égale à n et p. Puisque α_2 est bijective, on peut retrouver n et p à partir de $\alpha_2(p,n)$ à l'aide des fonctions suivantes :

$$\beta_2^1(x) = \mu z \leqslant x\,(\exists t \leqslant x\ \alpha_2(z,t) = x) \text{ et } \beta_2^2(x) = \mu z \leqslant x\,(\exists t \leqslant x\ \alpha_2(t,z) = x),$$

et nous voyons que les fonctions β_2^1 et β_2^2 sont récursives primitives.

On peut alors définir α_3 par $\alpha_3(x,y,z) = \alpha_2(x,\alpha_2(y,z))$

et $$\beta_3^1 = \beta_2^1\ ,\ \beta_3^2 = \beta_2^1 \circ \beta_2^2\ ,\ \beta_3^3 = \beta_2^2 \circ \beta_2^2\ ,$$

et plus généralement

$$\alpha_{p+1}(x_1,x_2,\ldots,x_p,x_{p+1}) = \alpha_p(x_1,x_2,\ldots x_{p-1},\alpha_2(x_p,x_{p+1}))\ ;$$

$$\beta_{p+1}^1 = \beta_p^1\ ,\ \beta_{p+1}^2 = \beta_p^2\ ,\ldots,\ \beta_{p+1}^{p-1} = \beta_p^{p-1}\ ,\ \beta_{p+1}^p = \beta_2^1 \circ \beta_p^p\ ,\ \beta_{p+1}^{p+1} = \beta_2^2 \circ \beta_p^p.$$

Pour compléter, on posera $\alpha_1(x) = x$ et $\beta_1^1(x) = x$.

☺

NOTATION : On notera $\mathscr{S}$ l'ensemble des suites finies d'entiers ($\mathscr{S} = \mathscr{M}(\mathbb{N})$).

1.12 Dans l'exercice 3, on montre comment utiliser ces fonctions pour établir un codage de toutes les suites finies. En voici un autre, très classique, dont on se servira par la suite.

DEFINITION DE Ω ET δ : *La fonction* Ω *est l'application de* $\mathscr{S}$ *dans* $\mathbb{N}$ *définie comme suit :*

$$\Omega((x_0,x_1,\ldots,x_p)) = \pi(0)^{x_0}.\pi(1)^{x_1}\ldots\pi(p)^{x_p}$$

(rappelons que π *est la fonction qui à l'entier* n *fait correspondre le* (n + 1)*-ème nombre premier).*

On complétera cette définition en décidant que, si s *est la suite vide,* $\Omega(s) = 1$.

La fonction δ *est la fonction de* $\mathfrak{F}_2$ *définie comme suit :*

$$\delta(i,x) = \mu z \leqslant x \text{ (x n'est pas divisible par } \pi(i)^{z+1})$$

($\delta(i,x)$ *est l'exposant de* $\pi(i)$ *dans la décomposition de* x *en facteurs premiers).*

On remarque que la fonction δ est récursive primitive. Il n'est pas difficile de voir aussi que l'image de Ω (c'est-à-dire $\{x$; il existe $s \in \mathscr{S}$ tel que $x = \Omega(s)\}$) est l'ensemble $\mathbb{N} - \{0\}$. On n'a pas là un codage parfait puisque Ω n'est pas injective (il est clair que si $s,s' \in \mathscr{S}$, $\Omega(s) = \Omega(s')$ si et seulement si la plus longue des deux suites s ou s' est obtenue à partir de l'autre en ajoutant des zéros à la fin). On pourrait, d'ailleurs, la rendre injective en ajoutant un à chaque exposant, mais on perdrait la surjectivité. D'autre part, Ω prend très rapidement des valeurs énormes, et est donc inutilisable pour des calculs autres que théoriques. Mais cela n'a pas d'importance pour l'usage que l'on veut en faire.

1.13 EXEMPLE : **Les récurrences doubles.** Soient $g, g' \in \mathfrak{F}_p$ et $h, h' \in \mathfrak{F}_{p+3}$, quatre fonctions. A l'aide de ces fonctions, on peut définir simultanément deux nouvelles fonctions f et f' de $\mathfrak{F}_{p+1}$ par les conditions :

$$f(x_1,x_2,\ldots,x_p,0) = g(x_1,x_2,\ldots,x_p) ;$$
$$f'(x_1,x_2,\ldots,x_p,0) = g'(x_1,x_2,\ldots,x_p) ;$$
$$f(x_1,x_2,\ldots,x_p,y+1) = h(x_1,x_2,\ldots,x_p,y,f(x_1,x_2,\ldots,x_p,y),f'(x_1,x_2,\ldots,x_p,y)) ;$$
$$f'(x_1,x_2,\ldots,x_p,y+1) = h'(x_1,x_2,\ldots,x_p,y,f(x_1,x_2,\ldots,x_p,y),f'(x_1,x_2,\ldots,x_p,y)).$$

Nous allons voir que, si g,g',h,h' sont toutes les quatre récursives primitives, il en est de même de f et f'. Pour cela, introduisons la fonction $k = \alpha_2(f,f')$. Cette fonction peut être définie par récurrence de la façon suivante :

$$k(x_1,x_2,\ldots,x_p,0) = \alpha_2(g(x_1,x_2,\ldots,x_p),g'(x_1,x_2,\ldots,x_p)) ;$$
$$k(x_1,x_2,\ldots,x_p,y+1) = \alpha_2(h(x_1,x_2,\ldots,x_p,y,\beta_2^1(k(x_1,x_2,\ldots,x_p,y)),\beta_2^2(k(x_1,x_2,\ldots,x_p,y))),$$
$$h'(x_1,x_2,\ldots,x_p,y,\beta_2^1(k(x_1,x_2,\ldots,x_p,y)),\beta_2^2(k(x_1,x_2,\ldots,x_p,y)))).$$

La fonction k est donc récursive primitive et $f = \beta_2^1 o k$ et $f' = \beta_2^2 o k$ le sont aussi.

2. FONCTIONS RECURSIVES

La fonction d'Ackermann

2.1 Il s'agit dans cette sous-section de donner un exemple de fonction calculable au sens intuitif du terme, qui n'est pas récursive primitive, ce qui justifiera le travail supplémentaire demandé au lecteur dans la suite. La fonction que nous allons définir et que nous appellerons **la fonction d'Ackermann**, bien que ce soit une légère variante de la fonction originellement définie par Ackermann, est une fonction à deux variables que nous noterons ξ et qui est définie comme suit :

i) pour tout entier x, $\xi(0,x) = 2^x$;

ii) pour tout entier y, $\xi(y,0) = 1$;

iii) pour tous entiers x et y, $\xi(y + 1,x + 1) = \xi(y,\xi(y + 1,x))$.

Pour chaque entier n, appelons ξ_n la fonction $\lambda x.\xi(n,x)$. Alors $\xi_0(x) = 2^x$, et on voit facilement, à partir de la clause iii) ci-dessus, que, pour tout n positif, ξ_n est définie par récurrence à partir de ξ_{n-1} par

$$\xi_n(0) = 1 \text{ et } \xi_n(x + 1) = \xi_{n-1}(\xi_n(x)).$$

Cela montre d'abord qu'il y a une seule fonction ξ satisfaisant les conditions imposées, et de plus, que toutes les fonctions ξ_n sont récursives primitives (faire une récurrence sur n). En revanche, rien ne nous permet d'affirmer que la fonction ξ elle-même l'est, et c'est heureux car on va montrer qu'elle ne l'est pas. Pourtant, on peut effectivement calculer $\xi(x,y)$ pour n'importe quelles valeurs de x et y, comme le lecteur peut s'en convaincre facilement. Il nous faut maintenant montrer quelques lemmes faciles mais ennuyeux concernant cette fonction ξ.

2.2 LEMME 1 : *Pour tout* n *et pour tout* x, $\xi_n(x) > x$.

☺ On va utiliser un raisonnement faisant intervenir deux récurrences emboîtées : par récurrence sur n, on montre que, pour tout x, $\xi_n(x) > x$. C'est clair pour $n = 0$. Fixons $n > 0$ et supposons l'assertion

$$\text{pour tout entier x, } \xi_{n-1}(x) > x$$

vraie. On montre alors l'assertion

$$\text{pour tout entier x, } \xi_n(x) > x.$$

Pour cela, on fait maintenant une récurrence sur x. C'est clair pour $x = 0$ puisque $\xi_n(0) = 1$. On suppose donc $\xi_n(x) > x$ et on va montrer $\xi_n(x + 1) > x + 1$. On sait que

$\xi_n(x+1)=\xi_{n-1}(\xi_n(x))$, et donc, par la première hypothèse de récurrence, on voit que :

$$\xi_n(x+1) > \xi_n(x) \text{ soit } \xi_n(x+1) \geqslant \xi_n(x)+1.$$

Or, d'après la seconde hypothèse de récurrence, $\xi_n(x) > x$. Le lemme en découle.
☺

LEMME 2 : *Pour tout entier* n, *la fonction* ξ_n *est strictement croissante.*

☹ C'est clair pour n égal à 0. Ensuite, cela découle immédiatement du lemme 1 et de la formule $\xi_n(x+1)=\xi_{n-1}(\xi_n(x))$.
☺

LEMME 3 : *Pour tout* $n \geqslant 1$ *et pour tout* x, $\xi_n(x) \geqslant \xi_{n-1}(x)$.

☹ C'est clair pour $x=0$. Pour $x+1$, puisque $\xi_n(x) \geqslant x+1$ et que ξ_{n-1} est croissante, $\xi_{n-1}(\xi_n(x)) \geqslant \xi_{n-1}(x+1)$, et il suffit d'appliquer la formule

$$\xi_n(x+1)=\xi_{n-1}(\xi_n(x)).$$

☺

Si k est un entier, notons ξ_n^k la fonction ξ_n itérée k fois (c'est-à-dire $\xi_n^0=\lambda x.x$, $\xi_n^1=\xi_n$, et $\xi_n^{k+1}=\xi_n\circ\xi_n^k$). Le lemme suivant est une collection d'évidences :

LEMME 4 : *Les fonctions* ξ_n^k *sont toutes strictement croissantes. De plus, pour tous* m, n, k, h *et* x, $\xi_n^k(x) < \xi_n^{k+1}(x)$ *et* $\xi_n^k(x) \geqslant x$, $\xi_n^k\circ\xi_n^h=\xi_n^{k+h}$ *et, si* $m \leqslant n$, $\xi_m^k(x) \leqslant \xi_n^k(x)$.

2.3 Donnons maintenant une définition :

DEFINITION : *Soient* $f \in \mathfrak{F}_1$ *et* $g \in \mathfrak{F}_p$. *On dit que* f ***domine*** g *s'il existe un entier* A *tel que pour tout* $(x_1,x_2,\ldots,x_p)$, $g(x_1,x_2,\ldots,x_p) \leqslant f(\sup(x_1,x_2,\ldots,x_p,A))$.

En particulier, lorsque f est strictement croissante, f domine g si et seulement si $g(x_1,x_2,\ldots,x_p) \leqslant f(\sup(x_1,x_2,\ldots,x_p))$ sauf pour un nombre fini de p-uples $(x_1,x_2,\ldots,x_p)$.

Appelons C_n l'ensemble des fonctions qui sont dominées par au moins une itérée de ξ_n :

$$C_n = \{ g \ ; \text{il existe } k \text{ tel que } \xi_n^k \text{ domine } g \}.$$

Il est bien clair que les fonctions suivantes appartiennent à C_0 : les fonctions projections P_p^i, les fonctions constantes, la fonction successeur S, la fonction $\lambda x_1 x_2 \ldots x_p.\sup(x_1,x_2,\ldots,x_p)$, la fonction $\lambda xy.x + y$ et les fonctions $\lambda x.kx$ où k est un entier quelconque. De plus, la fonction ξ_n appartient à C_n. D'autre part, si f et g appartiennent toutes deux à $\mathfrak{F}_p$, si $g \in C_n$ et si pour tous $x_1,x_2,\ldots,x_p$, $f(x_1,x_2,\ldots,x_p) \leqslant g(x_1,x_2,\ldots,x_p)$, alors $f \in C_n$. Nous allons montrer :

LEMME 5 : *Pour tout entier* n, *l'ensemble* C_n *est clos par composition.*

☺ Soient $f_1,f_2,\ldots,f_m$ des fonctions à p variables de C_n et g une fonction à m variables de C_n. Il s'agit de montrer que $g(f_1,f_2,\ldots,f_m)$ est aussi dans C_n. On sait qu'il existe des entiers $A,A_1,A_2,\ldots,A_m,k,k_1,k_2,\ldots,k_m$ tels que, pour tous $y_1, y_2,\ldots, y_m$,

$$g(y_1,y_2,\ldots,y_m) \leqslant \xi_n^k(\sup(y_1,y_2,\ldots,y_m,A)),$$

et pour tous $x_1, x_2,\ldots, x_p$ et pour tout i compris entre 1 et m,

$$f_i(x_1,x_2,\ldots,x_p) \leqslant \xi_n^{k_i}(\sup(x_1,x_2,\ldots,x_p,A_i)).$$

Posons $B = \sup(A,A_1,A_2,\ldots,A_m)$ et $h = \sup(k_1,k_2,\ldots,k_m)$. En utilisant le lemme 4, on voit alors que, pour tous $x_1,x_2,\ldots,x_p$:

$$g(f_1(x_1,x_2,\ldots,x_p),f_2(x_1,x_2,\ldots,x_p),\ldots,f_m(x_1,x_2,\ldots,x_p)) \leqslant \xi_n^k(\xi_n^h(\sup(x_1,x_2,\ldots,x_p,B))),$$

et donc

$$g(f_1(x_1,x_2,\ldots,x_p),f_2(x_1,x_2,\ldots,x_p),\ldots,f_m(x_1,x_2,\ldots,x_p)) \leqslant \xi_n^{k+h}(\sup(x_1,x_2,\ldots,x_p,B)).$$

☺

LEMME 6 : *Pour tous entiers* n, k *et* x,

$$\xi_n^k(x) \leqslant \xi_{n+1}(x + k).$$

☺ Par récurrence sur k ; pour k égal à 0 ou 1, c'est clair. Si c'est vrai pour k, ça l'est pour $k + 1$:

$$\xi_n^{k+1}(x) = \xi_n(\xi_n^k(x)) \leqslant \xi_n(\xi_{n+1}(x + k)) = \xi_{n+1}(x + k + 1)$$

(l'inégalité découle de l'hypothèse de récurrence, la dernière égalité de la définition de ξ).

☺

LEMME 7 : *Soient* $g \in \mathfrak{F}_p$ *et* $h \in \mathfrak{F}_{p+2}$ *et on suppose de plus que* h *et* g *sont toutes deux dans* C_n $(n \geqslant 0)$. *Alors la fonction* f *définie par récurrence à partir de* g *et* h *appartient à* C_{n+1}.

☹ Traduisons les hypothèses. Tout d'abord la définition de f :

$$f(x_1,x_2,\dots,x_p,0) = g(x_1,x_2,\dots,x_p) \ ;$$
$$f(x_1,x_2,\dots,x_p,y+1) = h(x_1,x_2,\dots,x_p,y,f(x_1,x_2,\dots,x_p,y)) \ ;$$

ensuite les conditions de domination : il existe A_1, A_2, k_1, k_2 tels que, pour tous $x_1,x_2,\dots,x_p,y,z$,

$$g(x_1,x_2,\dots,x_p) \leqslant \xi_n^{k_1}(\sup(x_1,x_2,\dots,x_p,A_1)) \ ;$$
$$h(x_1,x_2,\dots,x_p,y,z) \leqslant \xi_n^{k_2}(\sup(x_1,x_2,\dots,x_p,y,z,A_2)).$$

On va maintenant montrer par récurrence sur y que, pour tous $x_1,x_2,\dots,x_p,y$:

$$(*) \qquad f(x_1,x_2,\dots,x_p,y) \leqslant \xi_n^{k_1+yk_2}(\sup(x_1,x_2,\dots,x_p,y,A_1,A_2)).$$

C'est clair pour $y = 0$; si c'est vrai pour y, ça l'est pour $y + 1$:

$$f(x_1,x_2,\dots,x_p,y+1) = h(x_1,x_2,\dots,x_p,y,f(x_1,x_2,\dots,x_p,y)) \ ;$$
$$f(x_1,x_2,\dots,x_p,y+1) \leqslant \xi_n^{k_2}(\sup(x_1,x_2,\dots,x_p,y,f(x_1,x_2,\dots,x_p,y),A_2)).$$

Donc, en utilisant l'hypothèse de récurrence (∗) et le lemme 4,

$$f(x_1,x_2,\dots,x_p,y+1) \leqslant \xi_n^{k_2}(\xi_n^{k_1+yk_2}(\sup(x_1,x_2,\dots,x_p,y,A_1,A_2))),$$

ce qui démontre notre assertion ; maintenant, en utilisant le lemme 6, on obtient

$$f(x_1,x_2,\dots,x_p,y) \leqslant \xi_{n+1}(\sup(x_1,x_2,\dots,x_p,y,A_1,A_2) + k_1 + k_2 y).$$

Or la fonction $\lambda x_1 x_2 \dots x_p y . \xi_{n+1}(\sup(x_1,x_2,\dots,x_p,y,A_1,A_2) + k_1 + k_2 y)$ s'obtient par composition à partir de fonctions de C_{n+1} ; elle est donc elle-même dans C_{n+1}, de même que f.

☺

Nous sommes maintenant en mesure d'énoncer :

2.4 COROLLAIRE : *L'ensemble* $\bigcup_{n \in \mathbf{N}} C_n$ *contient toutes les fonctions récursives primitives.*

☹ En effet, d'une part cet ensemble contient les fonctions constantes, les fonctions projections et la fonction successeur ; d'autre part, il est clos par composition et pour les définitions par récurrence.

☺

On en arrive au théorème principal de cette section :

THEOREME : *La fonction d'Ackermann n'est pas récursive primitive.*

☹ Raisonnons par l'absurde et supposons la fonction d'Ackermann récursive primitive ; il en est de même de la fonction $\lambda x.\xi(x,2x)$. Il existe donc des entiers n,k, et A tels que, pour tout $x > A$, $\xi(x,2x) \leqslant \xi_n^k(x)$. Donc pour tout $x > A$, on a :

$$\xi(x,2x) \leqslant \xi_n^k(x) \leqslant \xi_{n+1}(x + k) \quad \text{(lemme 6)},$$

et, si $x > \sup(A,k,n + 1)$, $\xi_{n+1}(x + k) < \xi_{n+1}(2x) < \xi_x(2x) = \xi(x,2x)$ (lemme 4), ce qui est absurde.

☺

En fait, on peut voir que la fonction $\lambda x.\xi(x,x)$ domine toutes les fonctions récursives primitives.

Le schéma μ et les fonctions partielles récursives

2.5 Il nous faut donc définir une classe plus large, que nous appellerons la classe des fonctions récursives. On le fera en admettant un nouveau schéma de définition, le schéma μ (non borné). L'idée est la suivante : soit A un sous-ensemble de $\mathbb{N}^{p+1}$; alors la fonction $f \in \mathfrak{F}_p$ que ce schéma μ permet de définir est la fonction qui à $(x_1,x_2,\dots,x_p)$ fait correspondre le plus petit entier z tel que $(x_1,x_2,\dots,x_p,z) \in A$. On voit tout de suite la difficulté : que se passe-t-il s'il n'existe pas d'entier z tel que $(x_1,x_2,\dots,x_p,z) \in A$? Il faut remarquer qu'il ne nous est pas possible de faire ce que l'on a fait pour le schéma μ borné et poser dans ce cas $f(x_1,x_2,\dots,x_p) = 0$. En effet, en admettant, ce que l'on doit faire, que l'on dispose d'un algorithme permettant de calculer la fonction caractéristique χ_A de A, la seule façon imaginable de calculer $f(x_1,x_2,\dots,x_p)$ est de calculer $\chi_A(x_1,x_2,\dots,x_p,0)$, s'arrêter si on trouve 1, sinon calculer $\chi_A(x_1,x_2,\dots,x_p,1)$, etc., jusqu'à tomber sur la valeur 1. Mais si pour tout entier z, $(x_1,x_2,\dots,x_p,z) \notin A$, alors le processus ne s'arrête pas, et on ne connaîtra jamais la valeur de $f(x_1,x_2,\dots,x_p)$. Autrement dit, on ne dispose pas d'algorithme pour calculer f, et on ne peut donc pas admettre ce schéma. Une possibilité serait de le restreindre au cas où, pour tout $(x_1,x_2,\dots,x_p)$, il existe z tel que $(x_1,x_2,\dots,x_p,z) \in A$ (on appellera ce schéma le **schéma μ total**). On obtiendrait, comme on le verra par la suite, toutes les fonctions récursives. Mais il est préférable de définir les fonctions récursives partielles ; la raison en est que les théorèmes d'énumération et de points fixes (théorème 3.18 et 4.14 de ce chapitre), essentiels dans cette matière, ne sont vrais que pour cette dernière classe (voir exercice 22).

Il s'agit donc de formaliser cette intuition ; pour commencer, donnons quelques définitions sur les fonctions partielles :

2.6 DEFINITION : *Une **fonction partielle de $\mathbb{N}^p$ dans $\mathbb{N}$** est un couple* (A,f) *où* $A \subseteq \mathbb{N}^p$ *et* f *est une application de* A *dans* $\mathbb{N}$ *;* A *est appelé le **domaine de définition** de la fonction.*

NOTATION : On notera $\mathfrak{F}_p^*$ l'ensemble des fonctions partielles de $\mathbb{N}^p$ dans $\mathbb{N}$, et $\mathfrak{F}^* = \bigcup_{p \geq 0} \mathfrak{F}_p^*$.

Si $(a_1,a_2,...,a_p) \notin A$, on dira que la fonction **n'est pas définie en** $(a_1,a_2,...,a_p)$, ou encore que $f(a_1,a_2,...,a_p)$ **n'est pas définie**. On n'hésitera pas à faire l'abus de langage consistant à confondre (A,f) avec f. Il faut insister sur le fait que deux fonctions partielles f et g sont égales si, premièrement, elles ont même domaine de définition, et deuxièmement, elles sont identiques sur ce domaine. Si le domaine d'une fonction partielle f de $\mathfrak{F}_p^*$ est $\mathbb{N}^p$ tout entier, on dit que f est **totale**. Le mot « fonction » restera réservé aux fonctions totales.

2.7 DEFINITION : *Soient* $f_1, f_2, ..., f_n \in \mathfrak{F}_p^*$ *et* $g \in \mathfrak{F}_n^*$. *La **fonction composée*** $h = g(f_1,f_2,...,f_n)$ *est l'élément de* $\mathfrak{F}_p^*$ *défini de la façon suivante :*

- $h(x_1,x_2,...,x_p)$ *n'est pas définie si l'une des* $f_i(x_1,x_2,...,x_p)$ *n'est pas définie ou si, toutes l'étant,* $g(f_1(x_1,x_2,...,x_p),f_2(x_1,x_2,...,x_p),...,f_n(x_1,x_2,...,x_p))$ *n'est pas définie.*
- *Dans le cas contraire,* $h(x_1,x_2,...,x_p)$ *est définie et est égale à :*

$$g(f_1(x_1,x_2,...,x_p),f_2(x_1,x_2,...,x_p),...,f_n(x_1,x_2,...,x_p)).$$

REMARQUE : Il faut se méfier des automatismes lorsqu'on travaille avec les fonctions partielles. Prenons par exemple deux fonctions f et g de $\mathfrak{F}_1^*$; il n'est pas toujours vrai que f et $(f + g) - g$ soient égales : si par exemple f est totale tandis que g n'est jamais définie, alors $(f + g) - g$ n'est jamais définie. Et, effectivement, un algorithme qui essaierait de calculer $(f + g) - g$ commencerait par calculer $f + g$ et n'y parviendrait jamais.

2.8 **Définition par récurrence** : On peut, pour les fonctions partielles, utiliser des définitions par récurrence grâce au fait suivant :

PROPOSITION : *Soient* $g \in \mathfrak{F}_p^*$ et $h \in \mathfrak{F}_{p+2}^*$. *Alors, il existe une et une seule fonction* $f \in \mathfrak{F}_{p+1}^*$ *vérifiant les conditions suivantes :*

• *Pour tout* $(x_1,x_2,\ldots,x_p) \in \mathbb{N}^p$, $f(x_1,x_2,\ldots,x_p,0) = g(x_1,x_2,\ldots,x_p)$ *(ce qui veut dire exactement :* $f(x_1,x_2,\ldots,x_p,0)$ *est définie si et seulement si* $g(x_1,x_2,\ldots,x_p)$ *l'est, et lui est égale dans ce cas).*

• *Pour tout* $(x_1,x_2,\ldots,x_p,y) \in \mathbb{N}^{p+1}$,

$$f(x_1,x_2,\ldots,x_p,y+1) = h(x_1,x_2,\ldots,x_p,y,f(x_1,x_2,\ldots,x_p,y))$$

(même remarque que précédemment : $f(x_1,x_2,\ldots,x_p,y+1)$ *est définie si et seulement si* $h(x_1,x_2,\ldots,x_p,y,f(x_1,x_2,\ldots,x_p,y))$ *l'est).*

On dira encore dans ce cas que f ***est définie par récurrence*** *à partir de* g et h.

2.9 DEFINITION : **Le schéma μ.** *Soit* $f \in \mathfrak{F}_{p+1}^*$. *Alors la fonction partielle*

$$g(x_1,x_2,\ldots,x_p) = \mu y(f(x_1,x_2,\ldots,x_p,y) = 0)$$

est définie de la façon suivante :

• *S'il existe au moins un entier* z *tel que* $f(x_1,x_2,\ldots,x_p,z)$ *soit nul et que, pour tout* $z' < z$, $f(x_1,x_2,\ldots,x_p,z')$ *soit définie, alors* $g(x_1,x_2,\ldots,x_p)$ *est le plus petit de ces entiers* z.

• *Dans le cas contraire,* $g(x_1,x_2,\ldots,x_p)$ *n'est pas définie.*

Si $A \subseteq \mathbb{N}^{p+1}$, *alors, par définition,*

$$\mu y((x_1,x_2,\ldots,x_p,y) \in A) = \mu y(1 \dot{-} \chi_A(x_1,x_2,\ldots,x_p,y) = 0).$$

Il faut prendre garde à ce que $z = \mu y(f(x_1,x_2,\ldots,x_p,y) = 0)$ implique que, pour tout y inférieur à z, $f(x_1,x_2,\ldots,x_p,y)$ est défini (et non nul). Premièrement, c'est la définition qu'il faut prendre si l'on veut suivre l'intuition de calculabilité effective (voir 3.9) ; deuxièmement, l'exercice 24 montre que négliger cette précaution conduirait à des catastrophes.

2.10 On peut maintenant définir l'ensemble des fonctions partielles récursives :

DEFINITION : *L'ensemble des* ***fonctions partielles récursives*** *est le plus petit sous-ensemble de* $\mathfrak{F}^*$ *qui*

• *contienne toutes les fonctions (totales) constantes, les projections* P_p^i *(pour* $1 \leqslant i \leqslant p$*), la fonction successeur* S,

• *soit clos pour la composition, les définitions par récurrence et le schéma* μ.
Un sous-ensemble A *de* $\mathbb{N}^p$ *est dit* ***récursif*** *si sa fonction caractéristique est (totale) récursive.*

On voit en particulier que les fonctions récursives primitives sont récursives (et même totales récursives). On vérifie aussi sans problème que les propriétés de clôture énoncées en 1.6, 1.7, 1.8 et 1.9 pour les fonctions récursives primitives sont encore vraies pour les fonctions partielles récursives et les fonctions totales récursives. On sait déjà que la fonction d'Ackermann n'est pas récursive primitive. Il faudra patienter jusqu'à la fin de ce chapitre, ou faire l'exercice 11, pour voir qu'elle est récursive, ce qui prouvera que la classe des fonctions récursives est strictement plus riche que celle des fonctions récursives primitives. Il est d'autre part aisé de construire une fonction partielle récursive qui n'est pas totale : par exemple la fonction partielle $f(x) = \mu y(2y = x)$ n'est définie que pour les nombres pairs. On donnera dans l'exercice 20 des exemples de fonctions récursives dont le caractère partiel est beaucoup plus définitif : il en existe qu'il est impossible de prolonger en une fonction totale récursive.

Le lecteur est invité à se persuader que les fonctions partielles récursives sont calculables dans le sens que nous avons mentionné dans l'introduction : pour chacune d'entre elles, il existe un algorithme qui, soit s'arrête au bout d'un temps fini en donnant la valeur de la fonction si celle-ci est définie au point considéré, soit ne se termine jamais dans le cas contraire. La section suivante montrera comment calculer mécaniquement une fonction partielle récursive.

2.11 Il reste le problème de la réciproque : une fonction calculable est-elle nécessairement récursive ? Autrement dit, avons-nous réussi dans notre tentative qui était de formaliser la notion de fonction calculable ? La réponse affirmative à cette question est ce qu'on appelle la **thèse de Church**. Il est clair que cette affirmation ne se prête pas à démonstration puisqu'on n'a pas de définition précise de ce qu'est une fonction calculable. D'autre part, l'échec de notre première tentative, celle des fonctions récursives primitives, doit nous rendre prudents. Mais en fait on ne connaît aucun contre-exemple à la thèse de Church, et, de plus, l'expérience montre que, chaque fois que l'on a une fonction que l'intuition dit être calculable, alors cette même intuition permet de donner une preuve qu'elle est récursive. En ce sens, les derniers théorèmes de ce chapitre (les théorèmes du point fixe) militent fortement en faveur de la thèse de Church.

3. MACHINES DE TURING

3.1 Les machines de Turing sont des machines théoriques qui sont capables de calculer, en un sens que l'on définira, certaines fonctions de $\mathfrak{F}_p^*$. Le fait important de cette section est qu'une fonction partielle est calculable par une machine de Turing si et seulement si elle est partielle récursive.

Description des machines de Turing

Une machine de Turing se compose

• d'un nombre fini de **bandes** disposées horizontalement, toutes bornées à gauche et infinies à droite ; chaque bande est divisée en cases successives;* les cases numéro 1 étant les cases les plus à gauche, suivies à droite par les cases numéro 2 etc. ; les bandes sont disposées de sorte que les cases d'un même numéro se trouvent sur une même verticale.

case n°1	case n°2		bande n°1
case n°1	case n°2		bande n°2
case n°1	case n°2		bande n°3

↑

tête de lecture

• d'une tête que nous appellerons **tête de lecture** mais qui peut lire, écrire ou effacer des symboles sur les bandes (à raison d'un symbole par case). La tête peut se déplacer horizontalement ; à chaque instant, elle est pointée sur une verticale, c'est-à-dire sur la série de cases d'un même numéro n correspondant aux différentes bandes et elle peut effectuer ces opérations (lecture, écriture, effacement) sur toutes ces cases. Les symboles que la tête peut écrire sont au nombre de trois : il y a le d qui est le symbole de début de bande, le bâton | et le blanc b. On notera $S = \{d, |, b\}$.

Cela est commun à toutes les machines de Turing. Maintenant, chaque machine est caractérisée par la donnée :

• du nombre n de ses bandes.

• d'un ensemble fini d'**états** E ; à chaque instant, la machine se trouvera dans un état donné. Il y a deux états particuliers qui appartiennent à toutes les machines : l'**état initial** e_i et l'**état final** e_f.

• d'une **table** M qui est une application de $S^n \times E$ dans $S^n \times E \times \{-1,0,+1\}$, quelquefois appelée **table de transition** de la machine.

3.2 La machine fonctionne en changeant d'état, en effaçant et écrivant sur les bandes et en déplaçant sa tête à chaque instant, en respectant les règles suivantes :

• à l'instant $t = 0$, la tête se trouve devant les cases numéro 1, sur lesquelles est écrit le symbole d ; un symbole est écrit sur chaque case de chaque bande. La machine se trouve dans l'état initial e_i ;

• à chaque instant t, la machine lit les symboles $s_1,s_2,\ldots,s_n$ inscrits sur les cases se trouvant devant sa tête ; la table M lui indique ce qu'elle doit faire : en supposant qu'elle se trouve dans l'état e et que $M(s_1,s_2,\ldots,s_n,e) = (s_1',s_2',\ldots,s_n',e',\varepsilon)$ où $\varepsilon \in \{-1,0,+1\}$, alors la machine efface les symboles $s_1,s_2,\ldots,s_n$, écrit $s_1',s_2',\ldots,s_n'$ à la place ; elle déplace sa tête d'une case vers la droite si $\varepsilon = +1$, vers la gauche si $\varepsilon = -1$, et ne bouge pas sa tête si $\varepsilon = 0$; enfin elle passe dans l'état e' ; l'instant t est alors écoulé et on passe à l'instant $t + 1$ et la machine recommence les mêmes opérations ;

• lorsque la machine atteint l'état final e_f, elle s'arrête de fonctionner.

Le bon fonctionnement de la machine exige que la table M satisfasse un certain nombre de contraintes :

• la machine doit s'arrêter de fonctionner aussitôt atteint l'état final ; cela se traduit par le fait que, pour tous $s_1,s_2,\ldots,s_n \in S^n$, $M(s_1,s_2,\ldots,s_n,e_f) = (s_1,s_2,\ldots,s_n,e_f,0)$;

• il n'est pas possible à la machine d'effacer ou d'écrire le symbole de début de bande ; d'autre part la tête ne peut aller à gauche lorsqu'elle lit le symbole d. Donc, pour tout e appartenant à E, $M(d,d,\ldots,d,e) = (d,d,\ldots d,e',\varepsilon)$ où e' appartient à E et ε est égal à 0 ou +1 ; si $(s_1,s_2,\ldots,s_n) \neq (d,d,\ldots,d)$ et $M(s_1,s_2,\ldots,s_n,e) = (s_1',s_2',\ldots s_n',e',\varepsilon)$, alors aucun des s_i' n'est égal à d.

On fera toujours implicitement l'hypothèse que ces conditions sont satisfaites. On supposera aussi que, à l'instant $t = 0$, il n'y a qu'un nombre fini de cases remplies par autre chose que le blanc, et que le symbole d se trouve en début de chaque bande et uniquement là. Ces hypothèses resteront vraies à tout instant. On remarque aussi que le fonctionnement de la machine est complètement déterminé : on peut prévoir ce qui sera écrit sur les bandes à l'instant t si on sait ce qui y est écrit à l'instant initial $t = 0$

On va maintenant voir comment une machine de Turing peut calculer une fonction partielle, et montrer que les fonctions partielles qui sont ainsi calculables sont exactement les fonctions partielles récursives.

Les fonctions T-calculables

3.3 Pour qu'une machine puisse calculer la valeur d'une fonction f en $(x_1,x_2,\ldots,x_p)$, il faut évidemment rentrer les valeurs des variables $(x_1,x_2,\ldots,x_p)$ d'une façon ou d'une autre. Cela se fera dans la configuration initiale. Pour calculer une fonction à p variables, il faut une machine possédant au moins $p + 1$ bandes : sur les p premières bandes sont rentrées les données, le résultat est codé sur la $(p + 1)$-ème bande, et les autres bandes (s'il y en a) servent aux calculs intermédiaires. Voyons d'abord comment coder un entier sur une bande :

DEFINITION : *On dira qu'une bande* **représente**, *à un instant donné, un entier* x, *si les symboles qui y sont écrits à cet instant sont :*

$$(d,\underbrace{|,|,\ldots,|}_{x\ \text{bâtons}},b,b,\ldots),$$

c'est-à-dire le symbole d *sur la première case, le bâton sur les cases numéro* $2,3,\ldots, x + 1$, *puis des blancs sur les suivantes. Une bande où zéro est représenté (donc où il y a un* d *suivi de blancs) sera appelée une bande* **blanche**.

3.4 DEFINITION : *Soient* f *une fonction partielle à* p *variables et* $\mathcal{M}$ *une machine de Turing possédant au moins* $p+1$ *bandes ; on dit que* $\mathcal{M}$ **calcule** f *si, pour toute suite d'entiers* $(x_1,x_2,\ldots,x_p)$, *si l'on fait fonctionner la machine* $\mathcal{M}$ *à partir d'une configuration initiale où, sur les bandes numéro* 1, 2, ..., p, *sont respectivement représentés les entiers* x_1, x_2, ..., x_p, *les autres bandes étant blanches, alors :*

• *si* $f(x_1,x_2,\ldots,x_p)$ *n'est pas définie, la machine ne s'arrête jamais (c'est-à-dire n'atteint jamais l'état final) ;*

• *si* $f(x_1,x_2,\ldots,x_p)$ *est définie, la machine s'arrêtera au bout d'un temps fini, et, à cet instant,* x_1 *sera représenté sur la première bande,* x_2 *sur la seconde, et ainsi de suite jusqu'à la* p*-ème et* $f(x_1,x_2,\ldots,x_p)$ *sur la* $(p + 1)$*-ème bande. Les éventuelles autres bandes doivent être blanches.*

On dit que $f \in \mathfrak{F}_p$ *est* **T-calculable** *(T pour Turing) s'il existe une machine* $\mathcal{M}$ *calculant* f.

REMARQUES : 1°) On exige de la machine qu'elle nettoie ses bandes de calcul avant de s'arrêter. Ce n'est pas vraiment nécessaire, mais cela aidera lorqu'on voudra faire

calculer à une machine une fonction définie par récurrence ou par composition.

2°) Il existe bien d'autres définitions possibles de machines de Turing : certaines n'ont qu'une seule bande, d'autres ont plus de symboles, etc. Elles sont toutes équivalentes en ce sens qu'elles calculent toutes exactement les mêmes fonctions partielles. La notion qui est présentée ici a été choisie car, nous semble-t-il, elle permet une démonstration pas trop compliquée du théorème fondamental de cette section, à savoir que les fonctions partielles récursives sont celles qui sont T-calculables, tout en minimisant les codages nécessaires.

3.5 Nous allons maintenant donner quelques exemples de fonctions T-calculables. A chaque fois, pour décrire la machine correspondante, il faudrait préciser le nombre de bandes, les états et la table. En fait, le plus souvent, seules les valeurs prises par la fonction M sur une partie de $S^n \times E$ sont utiles : certaines de ces valeurs sont imposées une fois pour toutes (voir 3.2) et d'autres ne vont jamais intervenir. On se bornera donc à donner la partie utile de M.

EXEMPLE : La fonction successeur est T-calculable ; on peut la calculer à l'aide d'une machine à deux bandes dont l'ensemble d'états est $\{e_i, e_f\}$. Voici la partie significative de sa table :

$M(d,d,e_i) = (d,d,e_i,+1)$;
$M(|,b,e_i) = (|,|,e_i,+1)$;
$M(b,b,e_i) = (b,|,e_f,0)$.

EXEMPLE : La fonction $\lambda x.2x$ est T-calculable : la machine n'aura toujours que deux bandes ; il y a quatre états, e_i, e_f, e_1 et e_2 ; elle fonctionnera de la façon suivante : elle va lire la première bande de gauche à droite et à chaque fois qu'elle lira un bâton, elle en écrira un sur la seconde bande et ira en écrire un autre en fin de mot, toujours sur la seconde bande. Voici sa table :

$M(d,d,e_i) = (d,d,e_i,+1)$ (démarrage) ;

$M(|,b,e_i) = (|,|,e_1,+1)$; $M(b,b,e_i) = (b,b,e_f,0)$ (on rajoute un premier bâton sur la deuxième bande, sauf, bien sûr, si x est égal à **0**) ;

$M(|,b,e_1) = (|,b,e_1,+1)$; $M(b,|,e_1) = (b,|,e_1,+1)$ (on va à la fin du mot) ;

$M(b,b,e_1) = (b,|,e_2,-1)$; (on rajoute un bâton) ;

$M(b,|,e_2) = (b,|,e_2,-1)$; $M(|,b,e_2) = (|,b,e_2,-1)$ (on revient sous le dernier bâton que l'on a dédoublé) ;

$M(|,|,e_2) = (|,|,e_i,+1)$; $M(b,|,e_i) = (b,|,e_f,0)$ (on recommence jusqu'à avoir dédoublé tous les bâtons).

3.6 En fait, il n'était pas indispensable de traiter l'exemple ci-dessus : on va maintenant montrer que, de façon générale, toutes les fonctions partielles récursives sont

T-calculables. Pour cela, il faut montrer que les fonctions constantes, les projections et la fonction successeur sont T-calculables, et que l'ensemble des fonctions T-calculables est clos pour la composition, les définitions par récurrence et le schéma μ. Le cas de la fonction successeur est déjà traité.

• Commençons par la projection P_p^i. Une machine qui calcule cette fonction peut être facilement décrite ; elle a $p+1$ bandes, deux états e_i et e_f et voici sa table M :

$M(d,d,\ldots,d,e_i) = (d,d,\ldots,d,e_i,+1)$;

$M(s_1,s_2,\ldots,s_p,b,e_i) = (s_1,s_2,\ldots,s_p,|,e_i,+1)$ si $s_i = |$;

$M(s_1,s_2,\ldots,s_p,b,e_i) = (s_1,s_2,\ldots,s_p,b,e_f,0)$ si $s_i = b$.

• Les fonctions constantes sont aussi T-calculables ; décrivons la machine calculant la fonction à p variables constante égale à k. Cette machine a $p + 1$ bandes et $k + 2$ états $e_i,e_f,e_1,e_2,\ldots,e_k$; sa table est donnée par :

$M(d,d,\ldots,d,e_i) = (d,d,\ldots,d,e_1,+1)$;

$M(s_1,s_2,\ldots,s_p,b,e_n) = (s_1,s_2,\ldots,s_p,|,e_{n+1},+1)$ pour tous $s_1,s_2,\ldots,s_p$ et pour tout n compris entre 1 et $k-1$;

$M(s_1,s_2,\ldots,s_p,b,e_k) = (s_1,s_2,\ldots,s_p,|,e_f,0)$ pour tous $s_1,s_2,\ldots,s_p$.

3.7 Il faut maintenant montrer que l'ensemble des fonctions partielles T-calculables est clos pour la composition, les définitions par récurrence et le schéma μ. Commençons par la composition : soient donc $f_1,f_2,\ldots,f_n$ des fonctions de $\mathfrak{F}_p^*$ et $g \in \mathfrak{F}_n^*$, et on suppose que toutes ces fonctions sont T-calculables. Il s'agit de construire une machine de Turing $\mathcal{M}$ qui calcule la fonction partielle $h = g(f_1,f_2,\ldots,f_n)$. On sait que pour i compris entre 1 et n, il existe une machine $\mathcal{M}_i$ calculant f_i ; on suppose que cette machine a p_i bandes ($p_i \geqslant p + 1$) et que son ensemble d'états est E_i. Quitte à renommer les éléments des E_i, on peut supposer que les ensembles E_i sont deux à deux disjoints (donc ont des états initiaux et finaux différents). La fonction g est aussi calculable par une machine $\mathcal{N}$; cette machine a n' bandes, son ensemble d'états est E ; on supposera aussi que E est disjoint de tous les E_i. L'ensemble d'états de la machine $\mathcal{M}$ est $E \cup (\bigcup_{1\leqslant i\leqslant n} E_i)$; son état initial est l'état initial de $\mathcal{M}_1$ et son état final est l'état final de $\mathcal{N}$. Le nombre de bandes de $\mathcal{M}$ est $p' = p + \Sigma_{i=1}^{i=n}(p_i - p) + n'-n$. On se contentera de décrire le fonctionnement de cette machine $\mathcal{M}$ calculant h, laissant au lecteur le soin d'établir, s'il le désire, sa table exacte.

On suppose donc qu'à l'instant $t = 0$, les entiers $x_1,x_2,\ldots,x_p$ sont représentés sur les p premières bandes et que les autres bandes sont blanches. La machine commence à calculer $f_1(x_1,x_2,\ldots,x_p)$ en travaillant comme $\mathcal{M}_1$, à ceci près qu'elle ne se sert pas de la bande numero $p + 1$. Elle utilise pour cela p_1 des p' bandes qu'elle a à sa disposition (les p premières et $p_1 - p$ autres) en ignorant les autres. Lorsqu'elle a fini son calcul (si jamais elle le finit), les entiers $x_1,x_2,\ldots,x_p$ restent representés sur les p premières bandes

et le résultat $f_1(x_1,x_2,...,x_p)$ est représenté sur une autre bande que nous appellerons B_1. L'état final de la première machine ramène la tête en début de bande, et lorsque celle-ci lit la suite de d, elle met $\mathcal{M}$ dans l'état initial de $\mathcal{M}_2$. En utilisant les p premières bandes plus $p_2 - p$ nouvelles bandes, elle va maintenant calculer $f_2(x_1,x_2,...,x_p)$ qui sera donc représenté à la fin du calcul (si fin il y a) sur une bande que nous appellerons B_2 ; après quoi elle remettra sa tête en début de bande et calculera $f_3(x_1,x_2,...,x_p)$ et ainsi de suite. La seule chose à laquelle il faille veiller est de ne pas se servir de la bande numéro $p + 1$ pour y écrire un des résultats intermédiaires $f_i(x_1,x_2,...,x_p)$. Lorsque c'est terminé et que la tête est revenue en début de bande, $\mathcal{M}$ passe dans l'état initial de $\mathcal{N}$, et travaille comme le ferait $\mathcal{N}$, en se servant de B_1 (sur laquelle, rappelons-le est représenté $f_1(x_1,x_2,...,x_p)$) comme première bande, de B_2 comme deuxième bande, etc., et en se servant de la bande numéro $p + 1$ pour y écrire le résultat $h(x_1,x_2,...,x_p)$. Il ne reste plus qu'à effacer le contenu des bandes B_1, B_2, etc.

3.8 Voyons maintenant comment calculer une fonction définie par récurrence. Il s'agit donc de calculer la fonction partielle $f \in \mathfrak{F}^*_{p+1}$ définie par :

$$f(x_1,x_2,...,x_p,0) = g(x_1,x_2,...,x_p),$$
$$f(x_1,x_2,...,x_p,y + 1) = h(x_1,x_2,...,x_p,y,f(x_1,x_2,...,x_p,y)),$$

où $g \in \mathfrak{F}^*_p$ et $h \in \mathfrak{F}^*_{p+2}$ sont des fonctions partielles calculées par des machines $\mathcal{M}$ et $\mathcal{M}'$, respectivement. On supposera que les machines $\mathcal{M}$ et $\mathcal{M}'$ ont $p + 1 + k$ et $p + 3 + k'$ bandes, que leurs ensembles d'états sont E et E' et que E et E' sont disjoints. L'état final de $\mathcal{M}$ est e_f, celui de $\mathcal{M}'$ est e_g. La machine $\mathcal{N}$ qui va calculer f est une machine à $p + 4 + k + k'$ bandes. L'ensemble de ses états est $E \cup E' \cup \{e_0,e_1,e_2,e_3,e_4,e_5,e_6,e_7\}$ (où les e_i, pour i variant de 0 à 7, sont de nouveaux états n'appartenant pas déjà à $E \cup E'$) ; son état initial est l'état initial de la machine $\mathcal{M}$. Il faut donc construire cette machine $\mathcal{N}$ de telle sorte que, si les entiers $x_1,x_2,...,x_p$ et x_{p+1} sont représentés sur les bandes numéro 1, 2, $p + 1$ à l'instant $t = 0$, l'entier $f(x_1,x_2,...,x_p,x_{p+1})$ soit représenté sur la bande $p + 2$ à la fin du calcul. Voici comment elle fonctionne :

Pour commencer, elle va travailler comme $\mathcal{M}$, en utilisant les bandes $1,2,...,p,p + 4$ ainsi que k bandes de calcul. A la fin de cette première étape, il y a donc $g(x_1,x_2,...,x_p)$ représenté sur la bande numéro $p + 4$; ensuite, la tête est ramenée en début de bande ; $\mathcal{N}$ passe alors dans l'état e_0.

La machine va alors calculer successivement $f(x_1,x_2,...,x_p,1)$, $f(x_1,x_2,...,x_p,2)$, jusqu'à $f(x_1,x_2,...,x_p,x_{p+1})$. Lorsqu'elle est en train de calculer $f(x_1,x_2,...,x_p,y + 1)$, le nombre y est codé sur la bande $p + 2$ et la valeur de $f(x_1,x_2,...,x_p,y)$ est codée sur la bande $p + 3$: lorsqu'elle se trouve dans l'état e_0, elle transfère le contenu de la bande numéro $p + 4$ sur la bande $p + 3$ (en effaçant la bande numéro $p + 4$) et compare le contenu de la bande $p + 2$ avec celui de la bande $p + 1$ (où est inscrit x_{p+1}) : si elle voit que ces nombres sont égaux, elle efface le contenu de la bande $p + 2$ et s'arrête ; sinon

elle revient en début de bande et se met dans l'état initial de la machine $\mathscr{M}'$; ensuite elle fonctionne comme le ferait cette machine en se servant des bandes numéro $1,2,\ldots,p,p+2$ et $p+3$ comme bandes de données et de la bande numéro $p+4$ pour y écrire le résultat. Lorsque ce dernier calcul est terminé, elle ajoute un bâton à la bande $p+2$, replace sa tête en début de bande et se remet dans l'état e_0. Le lecteur que cela amuse pourra écrire la table N de la machine $\mathscr{N}$ et assigner à chacun des nouveaux états e_0 à e_7 un rôle précis.

3.9 Le schéma μ : on veut maintenant construire une machine $\mathscr{N}$ qui calcule $g(x_1,x_2,\ldots,x_p) = \mu y(f(x_1,x_2,\ldots,x_p,y) = 0)$, où f est elle-même une fonction partielle calculée par une machine $\mathscr{M}$. On va supposer que $\mathscr{M}$ a $p+2+k$ bandes et que son ensemble d'états est E. La machine $\mathscr{N}$ a aussi $p+2+k$ bandes, son ensemble d'états est $E \cup \{e_0,e_1,e_2,e_3,\}$ où e_0, e_1, e_2 et e_3 ne sont pas déjà dans E ; l'état initial de $\mathscr{N}$ est le même que celui de $\mathscr{M}$, et son état final est e_3.

Nous nous contenterons de décrire le fonctionnement de $\mathscr{N}$: elle commence à travailler exactement comme le ferait $\mathscr{M}$ avec les données $x_1,x_2,\ldots,0$; elle va donc écrire le nombre $f(x_1,x_2,\ldots,x_p,0)$ (si celui-ci est défini, évidemment) sur la bande numéro $p+2$; elle revient alors en début de bande et passe dans l'état e_0. Elle avance sa tête d'une case et examine ce qui est écrit sur la deuxième case de la bande $p+2$: si c'est un b, le calcul est terminé et elle passe dans l'état e_3. Sinon elle passe dans l'état e_1 qui lui fait remplacer le premier blanc qu'elle trouve sur la bande $p+1$ par un bâton ; elle passe alors dans l'état e_2 qui ramène sa tête en début de bande et la remet dans l'état initial de $\mathscr{M}$. La machine calculera donc successivement $f(x_1,x_2,\ldots,x_p,0)$, $f(x_1,x_2,\ldots,x_p,1)$ etc. et ne s'arrêtera que lorsqu'elle aura trouvé 0.

3.10 Nous venons donc de terminer la démonstration du théorème suivant :

THEOREME : *Toutes les fonctions partielles récursives sont* T-*calculables.*

REMARQUE : Il faut bien se persuader que les machines que nous avons décrites pour calculer les fonctions partielles définies par composition, par récurrence ou par le schéma μ ne se contentent pas de calculer la valeur de ces fonctions lorsqu'elles sont définies ; elles ont aussi la propriété de ne pas s'arrêter lorsque la fonction en question n'est pas définie.

Les fonctions partielles T-calculables sont récursives

3.11 Pour cette sous-section et les trois suivantes, on fixe une machine de Turing $\mathcal{M}$ et on va supposer que $\mathcal{M}$ calcule une fonction partielle $f \in \mathfrak{F}_p^*$. Pour montrer que, dans ces conditions, f est récursive, on va d'abord coder la situation dans laquelle se trouve $\mathcal{M}$ à l'instant t par un entier et montrer que ce code est une fonction récursive primitive de t et des conditions initiales. On aura besoin des fonctions α_n introduites en 1.11.

Il est bien clair que le nom des états n'a pas d'importance. Quitte à les renommer, on peut supposer que l'ensemble des états est $\{0,1,2,...,m\}$. Pour fixer les idées, disons que l'état initial est **0** tandis que **1** est l'état final. En outre, on identifie le symbole blanc avec **0**, le symbole de début de bande d avec **1** et le bâton avec **2**.

DEFINITION : *Supposons que* $\mathcal{M}$ *possède* n *bandes. On appelle* ***configuration de*** $\mathcal{M}$ ***à l'instant*** t *la suite infinie* $C(t) = (s_0,s_1,...,s_i,...)$ *où, pour tous* u *et* v $(0 \leqslant v < n)$, s_{nu+v} *est le symbole écrit sur la case numéro* $u+1$ *de la bande numéro* $v+1$ (s_i *est donc un entier compris entre* **0** *et* **2**). *La* ***situation de la machine à l'instant*** t *est le triplet* $S(t) = (e,k,C(t))$, *où* e *est l'état où se trouve la machine à l'instant* t, k *le numéro des cases se trouvant devant la tête, et* C(t) *la configuration de la machine.*

Autrement dit, C(t) est la suite obtenue en mettant bout à bout les suites $\sigma_1,\sigma_2,...,\sigma_i...$, où σ_i est la suite $(t_i^1,t_i^2,...,t_i^n)$, t_i^j étant le symbole écrit sur la case numéro i de la bande numéro j. On a déjà remarqué que cette suite infinie n'a qu'un nombre fini de termes non blancs (ou non nuls). Les suites infinies de symboles n'ayant qu'un nombre fini de termes non nuls seront codées de la façon suivante : à $C = (s_0,s_1,...,s_i,...)$, on fera correspondre le code

$$\Gamma(C) = \sum_{i \geqslant 0} s_i.3^i.$$

On utilisera ce même codage pour les suites finies : à $C = (s_0,s_1,...,s_q)$, on fait correspondre

$$\Gamma(C) = \sum_{0 \leqslant i \leqslant q} s_i.3^i.$$

Si on connaît le code $\Gamma(C)$ de la configuration C, on peut facilement retrouver le symbole écrit sur une case quelconque des bandes : désignons respectivement par q(x,y) et r(x,y) le quotient et le reste de la division euclidienne de x par y (si $y = 0$, on posera arbitrairement $q(x,y) = r(x,y) = 0$). Le symbole écrit sur la case numéro u de la bande numéro v est

$$r(q(\Gamma(C),3^{n(u-1)+v-1}),3).$$

On peut tout aussi facilement retrouver la suite σ des n symboles écrits sur les cases numéros u des différentes bandes : posons

$$\varepsilon(x,y,z) = r(q(x,3^{z(y-1)}),3^z).$$

Alors, le code $\Gamma(\sigma)$ de la suite σ est :

$$\Gamma(\sigma) = \varepsilon(\Gamma(C),u,n).$$

La situation $S = (e,k,C)$ de la machine sera codée par l'entier

$$\Gamma(S) = \alpha_3(e,k,\Gamma(C)).$$

3.12 Le lemme suivant est l'expression du fait que l'on peut déduire la situation de la machine à l'instant t + 1 si on connaît sa situation à l'instant t.

LEMME : *Il existe une fonction récursive primitive* $g \in \mathfrak{F}_1$ *telle que, si* x *est le code de la situation de la machine à l'instant* t, *alors* g(x) *est le code de la situation de la machine à l'instant* t + 1.

⊖ La fonction g est définie par cas (exactement $3^n.(m + 1) + 1$ cas) : pour chaque suite $\sigma = (s_0,s_1,...,s_{n-1})$ d'éléments de $\{0,1,2\}$ et chaque $j \in \{0,1,...,m\}$, on va décrire ce qui se passe si à l'instant t la machine lit la suite σ et se trouve dans l'état j :

L'état où se trouve la machine, le numéro des cases observées et le code de la configuration des bandes sont respectivement $\beta_3^1(x)$, $\beta_3^2(x)$ et $\beta_3^3(x)$. Le code de la suite que la tête est en train de lire est $\varepsilon(\beta_3^3(x),\beta_3^2(x),n) = c$.

Pour chaque c compris entre 0 et $3^n - 1$ (ce sont les valeurs que peut prendre $\Gamma(\sigma)$ si σ est une suite de symboles de longueur n), et pour chaque j compris entre 0 et m :

• Si $\beta_3^1(x) = j$, si $\varepsilon(\beta_3^3(x),\beta_3^2(x),n) = c$, si $\Gamma(s_0,s_1,...,s_{n-1}) = c$ (autrement dit, pour chaque i compris entre 0 et n - 1, on pose $s_i = r(q(c,3^i),3) = \varepsilon(c,i + 1,1)$), si $M(s_0,s_1...,s_{n-1},j) = (t_0,t_1...,t_{n-1},h,\omega)$ (et par conséquent les t_i seront compris entre 0 et 2, h sera compris entre 0 et m et ω entre -1 et + 1) et si $\Gamma(t_0,t_1,...,t_{n-1}) = c'$, alors :

le nouvel état sera h ;

la nouvelle position de la tête sera $\beta_3^2(x) + \omega$;

la nouvelle configuration ne diffère de l'ancienne que sur les cases numéro $\beta_3^2(x)$ (qui correspondent, dans la configuration de $\mathcal{M}$, aux indices compris entre $n(\beta_3^2(x) - 1)$ et $n(\beta_3^2(x) - 1) + n - 1$) où les t_i remplaceront les s_i. Son nouveau code sera donc :

$$\beta_3^3(x) + 3^{n.(\beta_3^2(x)-1)}(c' - c) ;$$

et, en récapitulant,

$$g(x) = \alpha_3(h,\beta_3^2(x) + \omega,\beta_3^3(x) + 3^{n.(\beta_3^2(x)-1)}(c' - c)).$$

• Si $\beta_3^1(x) > m$ ou si $\varepsilon(\beta_3^3(x),\beta_3^2(x),n)$ est strictement supérieur à $3^n - 1$ (cas qui ne se produira pas si x est réellement le code d'une situation), on pose arbitrairement $g(x) = 0$.

La fonction g que l'on vient de définir est bien récursive primitive parce qu'elle est définie par cas en utilisant des fonctions récursives primitives et des ensembles récursifs primitifs. La fonction M qui intervient dans la définition est complètement inoffensive.

☺

3.13 Démontrons maintenant le fait, intuitivement clair, que si on connaît la situation initiale de la machine, on peut en déduire sa situation à n'importe quel instant. Définissons la fonction $Sit(t,x_1,x_2,...,x_p)$ par récurrence en posant :

$Sit(0,x_1,x_2,...,x_p) = \alpha_3(0,1,\Gamma(C))$, C étant la configuration des bandes où x_1 est représenté sur la première bande, x_2 sur la seconde, etc. jusqu'à la p-ème bande sur laquelle x_p est représenté, les autres bandes étant blanches.

$$Sit(t + 1,x_1,x_2,...,x_p) = g(Sit(t,x_1,x_2,...,x_p)).$$

LEMME : *La fonction* $Sit(t,x_1,x_2,...,x_p)$ *est récursive primitive. Pour tous* $t,x_1,x_2,...,x_p$, $Sit(t,x_1,x_2,...,x_p)$ *est égale au code* $\Gamma(S)$ *de la situation de la machine* $\mathcal{M}$ *à l'instant* t, *en supposant qu'à l'instant* $t = 0$, *les entiers* $x_1,x_2,...,x_p$ *étaient représentés sur les bandes* $1,2,...,p$, *les autres bandes étant blanches.*

☺ Avec ce que l'on vient de voir, il suffit de montrer que $Sit(0,x_1,x_2,...,x_p)$ est une fonction récursive primitive de $x_1,x_2,...,x_p$. Or :

$$Sit(0,x_1,x_2,...,x_p) = \alpha_3(0,1,\Gamma(C)) ;$$

où C est la configuration initiale des bandes. Il suffit donc de voir que $\Gamma(C)$ est une fonction récursive primitive de $x_1,x_2,...,x_p$. Notons :

$\rho(i,x)$ la fonction égale à 2 si $i \leqslant x$ et à 0 sinon.

Alors, si $C = (s_0,s_1,...,s_i...)$ est la configuration initiale de la machine, s_i est le symbole écrit sur la bande numéro $r(i,n) + 1$, en $q(i,n)$-ème position. On a donc :

$s_i = 1$ si $0 \leqslant i \leqslant n - 1$

et $s_i = \rho(q(i,n),x_{r(i,n)+1})$ si $i \geqslant n$;

donc la fonction $\lambda i x_1 x_2 ... x_p . s_i$ est une fonction récursive primitive de même que $\Gamma(C)$ qui est égale à $\Sigma_{i=0}^{i=(n+1).sup(x_1,x_2,...,x_p)} 3^i.s_i$.

☺

On peut maintenant terminer la démonstration et montrer que f, la fonction que calcule la machine $\mathcal{M}$, est une fonction partielle récursive : $f(x_1,x_2,\ldots,x_p)$ est égale, si elle est définie, au nombre de bâtons se trouvant sur la bande numéro $p+1$ lorsque la machine a terminé son calcul. On trouve d'abord le **temps de calcul** (le premier instant où la machine atteint l'état final) :

$$T(x_1,x_2,\ldots,x_p) = \mu t(\beta_3^1(\mathrm{Sit}(t,x_1,x_2,\ldots,x_p)) = 1),$$

qui est donc défini si et seulement si $f(x_1,x_2,\ldots,x_p)$ est elle-même définie ; connaissant la situation de la machine à cet instant $T(x_1,x_2,\ldots,x_p)$, il est n'est pas difficile de compter le nombre de bâtons se trouvant sur la bande numéro $p+1$. Introduisons la fonction α :

$$\alpha(x) = \mu y(r(q(\beta_3^3(x),3^{n(y+1)+p}),3) = 0)$$

(en effet, si x est le code de la situation de la machine, $r(q(\beta_3^3(x),3^{n(y+1)+p}),3) = 0$ signifie que le symbole se trouvant sur la case $y+2$ est un blanc ; n'oublions pas que la première case est occupée par un d). On voit donc que $\alpha(x)$ est bien le nombre de bâtons consécutifs se trouvant au début de la bande numéro $p+1$.

On peut maintenant calculer f :

$$f(x_1,x_2,\ldots,x_p) = \alpha(\mathrm{Sit}(T(x_1,x_2,\ldots,x_p),x_1,x_2,\ldots,x_p)).$$

3.14 On peut donc énoncer :

THEOREME : *Si* f *est une fonction partielle qui est* T-*calculable, alors* f *est récursive.*

On peut remarquer que le seul endroit où l'on utilise le schéma μ non borné est la définition de la fonction T. En effet, un schéma μ borné est suffisant pour définir la fonction α qui est donc récursive primitive. Cela provient du fait que, si x est le code de la situation de la machine, il n'y a certainement pas plus de x bâtons écrits sur ses bandes. Donc

$$\alpha(x) = \mu y \leqslant x\ (r(q(\beta_3^3(x),3^{n(y+1)+p}),3) = 0).$$

Dans les sous-sections suivantes nous exploiterons plus profondément les possibilités du raisonnement qui vient d'être fait. On se contentera pour l'instant de remarquer deux ou trois choses qui peuvent être déduites de la façon dont f est écrite quelques lignes plus haut :

• Si la fonction $f \in \mathfrak{F}_p$ est une fonction calculable par une machine de Turing en un temps $T(x_1,x_2,\ldots,x_p)$ qui est une fonction récursive primitive, alors la fonction f est elle-même récursive primitive.

• On voit aussi que l'ensemble des fonctions partielles récursives est égal au plus petit sous-ensemble $\mathcal{A}$ de $\mathfrak{F}^*$ contenant les fonctions récursives primitives et clos pour la composition et le schéma μ (autrement dit, les définitions par récurrence ne sont plus

nécessaires si on a déjà toutes les fonctions récursives primitives) : soit en effet $\mathcal{M}$ une machine de Turing calculant une fonction partielle $f \in \mathfrak{F}_p^*$; la fonction partielle T que l'on vient de définir appartient visiblement à $\mathcal{A}$ (la fonction Sit est récursive primitive). de même que f qui s'obtient à l'aide de T et de fonctions récursives primitives.

• Considérons maintenant le plus petit sous-ensemble $\mathcal{B}$ de $\mathfrak{F}$ contenant les fonctions récursives primitives et clos pour la composition et le schéma μ total (c'est-à-dire que le schéma μ ne peut être utilisé que s'il définit une fonction totale). Cet ensemble est exactement égal à l'ensemble des fonctions totales récursives : si f est une fonction totale récursive calculée par une machine $\mathcal{M}$, la fonction T qui lui correspond appartient à $\mathcal{B}$, et on voit que f aussi.

Machines de Turing universelles

3.15 Jusqu'à présent, on a construit une machine de Turing pour chaque fonction partielle récursive que l'on voulait calculer. On va voir maintenant qu'il existe une machine de Turing qui est capable de calculer toutes les fonctions partielles récursives (à un nombre fixé de variables, mais ceci n'est pas bien gênant puisque l'on sait coder une fonction partielle de $\mathfrak{F}_p^*$ par une fonction partielle de $\mathfrak{F}_1^*$ au moyen de la fonction α_p). L'idée est de construire une machine à laquelle on fournirait, en plus de la valeur des variables, les instructions qu'elle devra suivre, qui sont en fait contenues dans la table de transition. On commencera plutôt par construire une fonction récursive universelle (dans un sens qui sera clair à la fin de cette section). Pour cela, il est indispensable d'établir un codage des machines de Turing.

On a déjà dit qu'une machine de Turing était définie par :

• le nombre n de ses bandes ;

• l'ensemble E de ses états, que l'on supposera encore être de la forme $\{0,1,\ldots,m\}$, avec toujours 0 comme état initial et 1 comme état final ;

• sa table de transition M : c'est une application de $S^n \times E$ dans $S^n \times E \times \{-1,0,+1\}$, c'est-à-dire d'un ensemble fini dans un ensemble fini. Il est tout-à-fait possible, bien qu'un peu compliqué, de coder cette application par un entier. Pour chaque suite $\rho = (s_1,s_2,\ldots,s_n,e)$ de $S^n \times E$, définissons successivement :

$$r_1 = \alpha_2(\Gamma(s_1,s_2,\ldots,s_n),e) \ ;$$
$$r_2 = \alpha_3(\Gamma(t_1,t_2,\ldots,t_n),e',\varepsilon + 1), \ \text{où } (t_1,t_2,\ldots,t_n,e',\varepsilon) = M(\rho) \ ;$$
$$n(\rho) = [\pi(r_1)]^{r_2}.$$

(Rappel : $\pi(i)$ est le $(i + 1)$-ème nombre premier.)

Le code de la table M sera l'entier u défini par :

$$u = \prod_{\rho \in S^n \times E} n(\rho).$$

Il est facile de retrouver M à partir de son code u : si on veut connaître

$$(t_1,t_2,\ldots,t_n,e',\varepsilon) = M(s_1,s_2,\ldots,s_n,e),$$

on calcule le code $c = \Gamma(s_1,s_2,\ldots,s_n)$ et $r = \alpha_2(c,e)$. On utilise ensuite la fonction δ introduite en 1.12 :

$$\delta(r,u) = \alpha_3(c',e',\varepsilon + 1), \text{ où } c' = \Gamma(t_1,t_2,\ldots,t_n),$$

et le décodage se termine alors sans difficulté.

3.16 Par définition, l'**indice** d'une machine $\mathcal{M}$ est l'entier $\alpha_3(n,m,u)$, où n est le nombre de bandes de $\mathcal{M}$, $m + 1$ le nombre de ses états, et u le code de sa table de transition. Il est bien clair que la condition « être l'indice d'une machine de Turing » est très restrictive, et que le premier entier à satisfaire cette condition est déjà très grand. Pour chaque entier p, on pose :

$I_p = \{x$; x est l'indice d'une machine de Turing ayant au moins $p + 1$ bandes$\}$.

Il serait horriblement ennuyeux, mais très facile, de vérifier que les ensembles I_p sont récursifs primitifs.

3.17 Définissons alors la fonction $ST^p(i,t,x_1,x_2,\ldots,x_p)$ par :

- Si $i \in I_p$, $ST^p(i,t,x_1,x_2,\ldots,x_p) = \Gamma(S(t))$ est le code à l'instant t de la situation de la machine d'indice i qui a commencé à fonctionner à l'instant $t = 0$ avec la configuration suivante : les entiers x_1, x_2,..., x_p sont représentés sur les bandes 1, 2, ...p, les autres bandes étant blanches (on remarque que ce code n'est jamais nul) ;
- $ST^p(i,t,x_1,x_2,\ldots,x_p) = 0$ sinon.

THEOREME : *Pour chaque entier* p, *la fonction* $ST^p(i,t,x_1,x_2,\ldots,x_p)$ *est récursive primitive.*

⊖ La fonction ST^p va être définie par cas suivant que i appartient à I_p ou non : si $i \notin I_p$, on pose évidemment $ST^p(i,t,x_1,x_2,\ldots,x_p) = 0$. C'est l'autre cas qui demande un peu plus de travail.

On voit sans grande difficulté qu'il existe une fonction récursive primitive $h(i,x_1,x_2,\ldots,x_p)$ qui, si i est l'indice d'une machine de Turing $\mathcal{M}$ ayant au moins $p + 1$ bandes, est le code de la situation initiale de $\mathcal{M}$, lorsque $x_1,x_2,\ldots,x_p$ sont représentés sur les bandes 1,2,...,p, les autres bandes étant blanches. Il suffit de reprendre les calculs du lemme 3.13 en remplaçant le nombre n par $\beta_3^1(i)$ (qui est le nombre de bandes de la machine d'indice i). Il n'y a pas à s'inquiéter de la valeur que prendra cette fonction (qui

est récursive primitive, donc toujours définie) si i n'est pas l'indice d'une machine de Turing ou si $\beta_3^1(i) < p + 1$.

Il faut ensuite montrer qu'il existe une fonction récursive primitive $g(i,x)$ telle que, si i est l'indice d'une machine $\mathcal{M}$ et x le code de la situation de $\mathcal{M}$ à l'instant t, alors $g(i,x)$ est le code de la situation de $\mathcal{M}$ à l'instant $t+1$. On s'inspire de la preuve de 3.12 ; toutefois on n'a même pas besoin de définition par cas. La suite σ de symboles que la tête est en train de lire a pour code $c = \varepsilon(\beta_3^3(x),\beta_3^2(x),\beta_3^1(i))$. Si c' est le code de la suite qui sera écrite à la place de σ, e' le nouvel état de la machine et ε ($=0,1$, ou -1) le déplacement de la tête, on a :

$$\alpha_3(c',e',\varepsilon+1) = \delta(\alpha_2(c,\beta_3^1(x)),\beta_3^3(i)).$$

Pour simplifier les notations, posons $\delta = \delta(\alpha_2(c,\beta_3^1(x)),\beta_3^3(i))$; alors

$$g(i,x) = \alpha_3(e',k',\Gamma(C')),$$

où :

$$e' = \beta_3^2(\delta) \;;$$
$$k' = \beta_3^2(x) + \beta_3^3(\delta) - 1 \;;$$
$$\Gamma(C') = \beta_3^3(x) + 3^{\beta_3^1(i)\,(\beta_3^2(x)\,-1)}(c' - c) \quad \text{où } c' = \beta_3^1(\delta).$$

⊖

On montre enfin par récurrence (comme en 3.13) que la situation d'une machine de Turing à l'instant t est une fonction récursive primitive de son indice, de la situation initiale et de t : $ST^p(i,t,x_1,x_2,\dots,x_p)$. Pour chaque entier p strictement positif, définissons la fonction partielle $\varphi^p(i,x_1,x_2,\dots,x_p)$ de la façon suivante :

- si $i \notin I_p$, $\varphi^p(i,x_1,x_2,\dots,x_p)$ n'est pas définie ;
- si $i \in I_p$, alors on fait fonctionner la machine d'indice i avec $x_1,x_2,\dots,x_p$ représentés sur ses bandes numéro 1, 2, ...,p, les autres bandes étant blanches et :
  - si cette machine ne s'arrête pas, alors on déclare que $\varphi^p(i,x_1,x_2,\dots,x_p)$ n'est pas définie ;
  - si elle s'arrête, alors $\varphi^p(i,x_1,x_2,\dots,x_p)$ est égal au nombre de bâtons consécutifs se trouvant au début de la bande numéro $p+1$.

3.18 THEOREME D'ENUMERATION : *Pour tout entier* $p > 0$, φ^p *est une fonction partielle récursive. De plus, si* f *est une fonction partielle récursive à* p *variables, il existe un entier* i *tel que :*

$$f = \lambda x_1x_2\dots x_p.\varphi^p(i,x_1,x_2,\dots,x_p).$$

⊖ La démonstration suit encore celle que l'on a faite en 3.13 ; on va introduire une fonction partielle récursive T^p et des prédicats récursifs primitifs B^p et C^p qui seront

utiles par la suite ; $T^p(i,x_1,x_2,...,x_p)$ est, lorsque $i \in I_p$, le temps de calcul de la machine d'indice i, celui-ci n'étant pas défini si cette machine ne s'arrête pas :

$$T^p(i,x_1,x_2,...,x_p) = \mu t(\beta_3^1(ST^p(i,t,x_1,x_2,...,x_p)) = 1)).$$

On remarque que, si $i \notin I_p$, $T^p(i,x_1,x_2,...,x_p)$ n'est pas défini. Pour chaque entier i, on pose :

$$B^p = \{ (i,t,x_1,x_2,...,x_p) \ ; \beta_3^1(ST^p(i,t,x_1,x_2,...,x_p)) = 1) \},$$

et $$B^p(i) = \{ (t,x_1,x_2,...,x_p) \ ; (i,t,x_1,x_2,...,x_p) \in B^p \}.$$

Ces ensembles sont récursifs primitifs et $(t,x_1,x_2,...,x_p) \in B^p(i)$ signifie (lorsque i est l'indice d'une machine de Turing) que cette machine que l'on a fait démarrer avec $x_1,x_2,...,x_p$ représentés sur ses p premières bandes, les autres bandes étant blanches, a terminé son calcul à l'instant t. On définit encore :

$C^p = \{ (i,y,t,x_1,x_2,...,x_p) \ ; \ i \in I_p, \ (i,t,x_1,x_2,...,x_p) \in B^p$ et le nombre de bâtons se trouvant à l'instant t sur la bande numéro $p + 1$ de la machine d'indice i que l'on a fait démarrer avec $x_1,x_2,...,x_p$ sur ses p premières bandes, les autres bandes étant blanches, est exactement $y \}$,

et $$C^p(i) = \{ (y,t,x_1,x_2,...,x_p) \ ; (i,t,x_1,x_2,...,x_p,y) \in C^p \}.$$

Il est encore très facile de voir que ces ensembles sont récursifs primitifs. On peut alors définir la fonction partielle φ^p comme suit :

$$\varphi^p(i,x_1,x_2,...,x_p) = \mu y((i,y,T^p(i,x_1,x_2,...,x_p),x_1,x_2,...,x_p) \in C^p),$$

ceci montre bien que φ^p est récursive.

☺

On peut, comme précédemment, améliorer un peu cette écriture pour mettre en évidence le fait que le seul endroit où l'on a besoin du schéma μ non borné est la définition de T^p ; en effet, le nombre de bâtons se trouvant sur une bande d'une machine de Turing est inférieur au code de la situation de cette machine. Posons

$$\psi(i,t,x_1,x_2,...,x_p) = \mu y \leqslant ST^p(i,t,x_1,x_2,...,x_p)[(i,t,x_1,x_2,...,x_p,y) \in C^p]$$

ψ est une fonction récursive primitive et

$$\varphi^p(i,x_1,x_2,...,x_p) = \psi(i,T(i,x_1,x_2,...,x_p),x_1,x_2,...,x_p).$$

3.19 La fonction partielle φ^p étant elle-même récursive, est calculable par une machine de Turing $\mathscr{M}$; cette machine peut donc calculer toutes les fonctions partielles récursives à p variables.

Pour chaque entier i, notons :

$$\varphi_i^p = \lambda x_1 x_2 ... x_p . \varphi^p(i,x_1,x_2,...,x_p).$$

On voit alors que l'ensemble $\{ \varphi_i^p \ ; i \in \mathbb{N} \}$ est égal à l'ensemble de toutes les fonctions partielles récursives à p variables.

DEFINITION : *Soit* $f \in \mathfrak{F}_p^*$ *une fonction partielle récursive. On dit que* $i \in \mathbb{N}$ *est un* ***indice*** *de* f *si* $f = \varphi_i^p$.

En particulier, si i est l'indice d'une machine de Turing calculant f, c'est aussi un indice de f ; mais il est clair, par exemple, que la fonction partielle de $\mathfrak{F}_p^*$ de domaine vide a aussi pour indice tous les entiers n'appartenant pas à I_p. Il peut aussi très bien arriver que j soit l'indice d'une machine $\mathcal{M}$ ayant au moins $p + 1$ bandes, mais que cette machine $\mathcal{M}$ ne calcule pas de fonction partielle de $\mathfrak{F}_p^*$, tout simplement parce que, lorsqu'elle s'arrête, ses bandes n'ont pas la configuration exigée par la définition 3.4 ; on a encore un exemple d'un entier i qui est l'indice d'une fonction f, bien que la machine d'indice i ne calcule pas la fonction f au sens strict du terme.

4. LES ENSEMBLES RECURSIVEMENT ENUMERABLES

Ensembles récursifs et récursivement énumérables

4.1 DEFINITION : *Soit* $A \subseteq \mathbb{N}^p$; *on dit que* A *est* ***récursif*** *si sa fonction caractéristique* χ_A *est (totale) récursive. On dit que* A *est* ***récursivement énumérable*** *si c'est le domaine de définition d'une fonction partielle récursive.*

On notera W_x^p le domaine de définition de la fonction partielle d'indice x (c'est-à-dire de φ_x^p). Il est clair que l'ensemble $\{W_x^p \; ; x \in \mathbb{N}\}$ est l'ensemble de tous les sous-ensembles récursivement énumérables de $\mathbb{N}^p$. Si $A = W_x^p$, on dira que x est un **indice** de A. On va montrer dans cette sous-section quelques faits simples sur les ensembles récursifs et récursivement énumérables.

• *Tout ensemble récursif est récursivement énumérable.*

☹ La fonction partielle $f = \mu y(y + 1 = x)$ est récursive, non définie en 0 et définie partout ailleurs. Si χ_A est la fonction caractéristique d'un ensemble récursif A, $f \circ \chi_A$ est une fonction partielle récursive et a pour domaine de définition l'ensemble A.

☺

• *Pour chaque entier* p, *l'ensemble des sous-ensembles récursifs de* $\mathbb{N}^p$ *est clos pour les opérations booléennes.*

☹ Même preuve que pour les ensembles récursifs primitifs.

☺

• *L'intersection et l'union de deux sous-ensembles récursivement énumérables de* $\mathbb{N}^p$ *sont récursivement énumérables.*

☹ Soient A_1 et A_2 deux sous-ensembles récursivement énumérables de $\mathbb{N}^p$, qui sont les domaines de définition des fonctions partielles f_1 et f_2 respectivement, calculées par des machines d'indices respectifs i_1 et i_2.

Il est d'abord clair que $A_1 \cap A_2$ est le domaine de définition de $f_1 + f_2$. D'autre part, $A_1 \cup A_2$ est le domaine de définition de la fonction partielle :

$$\mu t((t,x_1,x_2,\dots,x_p) \in B^p(i_1) \cup B^p(i_2))$$

(qui est récursive puisque les ensembles $B^p(i)$ (voir en 3.18) sont récursifs primitifs).

☺

4.2 Les trois propriétés qui suivent sont tellement importantes qu'on va leur donner le statut de :

THEOREME : *Soit* $A \subseteq \mathbb{N}^p$; A *est récursif si et seulement si* A *et* $\mathbb{N}^p - A$ *sont tous les deux récursivement énumérables.*

☹ Un sens est clair : si A est récursif, $\mathbb{N}^p - A$ est aussi récursif (4.1) et ces deux ensembles sont récursivement énumérables.

Soient i l'indice d'une machine calculant une fonction partielle de domaine A et i' celui d'une machine calculant une fonction partielle de domaine $\mathbb{N}^p - A$. Alors

$$h(x_1,x_2,\dots,x_p) = \mu t[(t,x_1,x_2,\dots,x_p) \in B^p(i) \cup B^p(i')]$$

est une fonction récursive totale et

$$(x_1,x_2,\dots,x_p) \in A \text{ si et seulement si } (h(x_1,x_2,\dots,x_p),x_1,x_2,\dots,x_p) \in B^p(i).$$

Si $\chi(t,x_1,x_2,\dots,x_p)$ est la fonction caractéristique de $B^p(i)$, celle de A est donc égale à

$$\chi(h(x_1,x_2,\dots,x_p),x_1,x_2,\dots,x_p),$$

ce qui montre bien que A est récursif.

☺

4.3 THEOREME : *La projection d'un ensemble récursivement énumérable est récursivement énumérable.*

Cela veut dire que, si $A \subseteq \mathbb{N}^{p+1}$ est récursivement énumérable, alors l'ensemble

$$B = \{ (x_1,x_2,\ldots,x_p) \ ; \text{il existe } x_0 \text{ tel que } (x_0,x_1,x_2,\ldots,x_p) \in A \}$$

est aussi récursivement énumérable.

☹ Soit i l'indice d'une machine de Turing calculant une fonction de domaine A. On voit alors que :

$(x_0,x_1,x_2,\ldots,x_p) \in A$ si et seulement si il existe un entier t tel que $(t,x_0,x_1,x_2,\ldots,x_p) \in B^p(i)$

et $(x_1,x_2,\ldots,x_p) \in B$ si et seulement si il existe des entiers t et x_0 tels que $(t,x_0,x_1,x_2,\ldots,x_p) \in B^p(i)$.

Cela montre que B est le domaine de définition de la fonction partielle récursive

$$g(x_1,x_2,\ldots,x_p) = \mu z((\beta_2^1(z),\beta_2^2(z),x_1,x_2,\ldots,x_p) \in B^p(i)).$$

☺

4.4 THEOREME : *Tout sous-ensemble récursivement énumérable de $\mathbb{N}^p$ est la projection d'un sous-ensemble récursif primitif de $\mathbb{N}^{p+1}$.*

☹ Ce qui veut dire que, si $A \subseteq \mathbb{N}^p$ est récursivement énumérable, il existe un ensemble $B \subseteq \mathbb{N}^{p+1}$ récursif primitif tel que :

$(x_1,x_2,\ldots,x_p) \in A$ si et seulement si il existe x_0 tel que $(x_0,x_1,x_2,\ldots,x_p) \in B$.

Il suffit de prendre pour B l'ensemble $B^p(i)$ défini en 3.18, où i est l'indice d'une machine de Turing calculant une fonction de domaine A.

☺

4.5 Voici quelques corollaires de ces théorèmes :

- *Le graphe d'une fonction partielle récursive est récursivement énumérable.*

☹ Soit $f \in \mathfrak{F}_p^*$; il s'agit de montrer que l'ensemble

$$G = \{ (x_1,x_2,\ldots,x_p,y) \ ; y = f(x_1,x_2,\ldots,x_p) \}$$

est récursivement énumérable.

Si i est l'indice d'une machine calculant f, on voit que $(x_1,x_2,\ldots,x_p,y) \in G$ si et seulement si il existe un entier t tel que $(y,t,x_1,x_2,\ldots,x_p) \in C^p(i)$, ce qui montre que G est la projection d'un ensemble récursif primitif et est donc récursivement énumérable.

☺

La réciproque est vraie : si le graphe G d'une fonction partielle f est récursivement énumérable, alors f est partielle récursive : il existe un ensemble récursif primitif A tel que $(x_1,x_2,...,x_p,y) \in G$ si et seulement si $\exists t\ (x_1,x_2,...,x_p,y,t) \in A$, et donc $f(x_1,x_2,...,x_p) = \beta_2^1(\ \mu t\ ((x_1,x_2,...,x_p,\beta_2^1(t),\beta_2^2(t)) \in A)\ )$.

L'image de f, c'est-à-dire l'ensemble des valeurs que prend f, est elle-même une projection du graphe de f ; donc :

• *L'image d'une fonction partielle récursive est récursivement énumérable.*

La réciproque est vraie ; on a même mieux :

• *Tout sous-ensemble récursivement énumérable non vide de* $\mathbb{N}$ *est l'image d'une fonction récursive primitive de* $\mathfrak{F}_1$.

☹ Soit A un sous-ensemble de $\mathbb{N}$ non vide et récursivement énumérable ; choisissons donc un entier $n \in A$ et soit i un indice de A. On a alors

$$x \in A \text{ si et seulement si il existe } t \text{ tel que } (t,x) \in B^1(i).$$

On vérifie facilement que A est l'image de la fonction récursive primitive g définie comme suit :

$$g(z) = \beta_2^2(z) \text{ si } (\beta_2^1(z),\beta_2^2(z)) \in B^1(i)\ ;$$
$$g(z) = n \text{ si } (\beta_2^1(z),\beta_2^2(z)) \notin B^1(i).$$

☺

4.6 Voici maintenant un point assez subtil qui est la généralisation de la définition par cas aux fonctions partielles récursives.

• *Soient* $g(x_1,x_2,...,x_p)$ *et* $g'(x_1,x_2,...,x_p)$ *deux fonctions partielles récursives, et* $A \subseteq \mathbb{N}^p$ *un ensemble récursif. Alors la fonction* f *définie par :*

$$f(x_1,x_2,...,x_p) = g(x_1,x_2,...,x_p) \textit{ si } (x_1,x_2,...,x_p) \in A$$

et $$f(x_1,x_2,...,x_p) = g'(x_1,x_2,...,x_p) \textit{ sinon}$$

est une fonction partielle récursive.

(Attention au sens exact de cette définition : si $(x_1,x_2,...,x_p) \in A$, alors $f(x_1,x_2,...,x_p)$ est définie si et seulement si $g(x_1,x_2,...,x_p)$ l'est, et dans ce cas ces deux valeurs sont égales ; même chose avec g' si $(x_1,x_2,...,x_p) \notin A$. On se convaincra que f n'est pas en général égale à $g.\chi(A) + g'.\chi(\mathbb{N}^p - A)$).

☹ Soient i et i' des indices pour g et g'. Considérons le sous-ensemble C de $\mathbb{N}^{p+2}$ suivant :

$$C = \{\ (y,t,x_1,x_2,...,x_p)\ \ ;\ [\ (y,t,x_1,x_2,...,x_p) \in C^p(i) \text{ et } (x_1,x_2,...,x_p) \in A\ ] \text{ ou }$$
$$[\ (y,t,x_1,x_2,...,x_p) \in C^p(i') \text{ et } (x_1,x_2,...,x_p) \notin A\ ]\ \}.$$

Cet ensemble est récursif ; $(y,t,x_1,x_2,\ldots,x_p) \in C$ signifie que : soit $(x_1,x_2,\ldots,x_p) \in A$ et la machine d'indice i a terminé son calcul à l'instant t et la valeur qu'elle trouve est y, soit $(x_1,x_2,\ldots,x_p) \notin A$ et la machine d'indice i' a terminé son calcul à l'instant t et la valeur qu'elle trouve est y. On voit donc que $f(x_1,x_2,\ldots,x_p)$ est égale au plus petit y tel qu'il existe t tel que $(y,t,x_1,x_2,\ldots,x_p) \in C$. Cela donne :

$$f(x_1,x_2,\ldots,x_p) = \beta_2^1[\mu z((\beta_2^1(z),\beta_2^2(z),x_1,x_2,\ldots,x_p) \in C)],$$

et on voit bien que f est partielle récursive.

☺

Le problème de l'arrêt

4.7 Nous avons jusqu'à présent soigneusement évité d'aborder un problème qui pourtant s'impose : existe-t-il des ensembles récursivement énumérables qui ne sont pas récursifs ? Avec ce que l'on sait déjà, cela revient à se demander s'il existe un ensemble récursivement énumérable dont le complémentaire n'est pas récursivement énumérable.

La réponse est oui : reprenons la fonction partielle à deux variables $\varphi^1(i,x)$; posons $g(x) = \varphi^1(x,x)$ et soit A le domaine de définition de g. Cet ensemble est certainement récursivement énumérable. Mais son complémentaire ne l'est pas. En effet, pour tout entier x, $x \in A$ si et seulement si $x \in W_x^1$. Supposons, pour obtenir une contradiction, qu'il existe un entier n tel que $\mathbb{N} - A = W_n^1$, c'est-à-dire tel que, pour tout entier x,

$$x \notin A \text{ si et seulement si } x \in W_n^1.$$

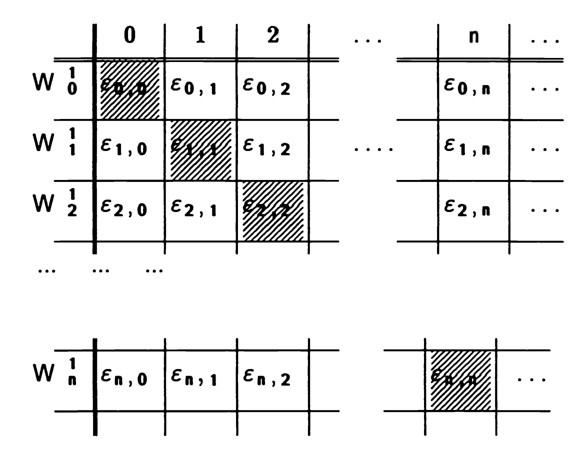
En choisissant x égal à n dans les deux équivalences ci-dessus, on obtient :

$$n \in A \text{ si et seulement si } n \in W_n^1,$$
$$n \notin A \text{ si et seulement si } n \in W_n^1,$$

ce qui est manifestement absurde.

Ce type de raisonnement, très populaire chez les logiciens, est connu sous le nom d'**argument diagonal**. On va en faire une analyse plus précise qui justifiera le mot diagonal : on a établi ci-dessous un tableau à double entrée rempli de zéros et de uns, dont chaque entrée est indexée par les entiers, de telle sorte que la suite écrite sur la première ligne soit la fonction caractéristique de W_0^1, celle écrite sur la seconde la fonction caractéristique de W_1^1, etc.

Dans ce tableau $\varepsilon_{p,n}$ est égal à 1 si $n \in W_p^1$ et à 0 sinon. On voit alors que la fonction caractéristique de l'ensemble A qui a été construit plus haut est obtenue en prenant la diagonale de ce tableau, et la suite correspondant à la fonction caractéristique du complémentaire de A est :



Si $\mathbb{N} - A$ était égal, pour un certain n, à W_n^1, alors la $(n + 1)$-ème ligne de ce tableau serait :

$$1 - \varepsilon_{0,0} \,,\, 1 - \varepsilon_{1,1} \,,\, \dots \,,\, 1 - \varepsilon_{n,n} \,,\, \dots$$

Mais à l'intersection de cette ligne avec la $(n + 1)$-ème colonne, (celle de l'entier n), qui se trouve aussi sur la diagonale, on devrait trouver à la fois $\varepsilon_{n,n}$ et $1 - \varepsilon_{n,n}$ ce qui est absurde.

4.8 COROLLAIRE : *L'ensemble* $\{(m,x) \;;\; \varphi^1(m,x)$ *est définie*$\}$ *n'est pas récursif.*

☺ En effet, si cet ensemble était récursif, il en serait de même de l'ensemble :

$$\{(x,x) \;;\; \varphi^1(x,x) \text{ est définie}\},$$

et on vient de voir que ce n'est pas le cas.

☺

L'intuition est qu'un ensemble $A \subseteq \mathbb{N}$ est récursif s'il existe un algorithme permettant de décider si un entier appartient ou non à A. Il est récursivement énumérable s'il existe un algorithme $\mathscr{A}$ qui permet d'énumérer A. Si A est récursivement énumérable et si on se demande si un entier donné n appartient ou non à A, on peut toujours faire tourner l'algorithme $\mathscr{A}$. Si, à un moment donné, l'entier n apparaît dans la suite énumérée par $\mathscr{A}$, alors on est sûr que $n \in A$. En revanche, on ne peut rien dire tant qu'il n'est pas apparu.

Le corollaire précédent exprime donc que la donnée de l'indice d'une machine de Turing (qui intuitivement représente les instructions) et de la configuration initiale, ne

permet pas de savoir effectivement si cette machine va s'arrêter ou non. C'est ce qu'on traduit en disant que le problème de l'arrêt d'une machine de Turing est indécidable.

Il y a un grand nombre de problèmes pour lesquels il est intéressant de savoir s'ils sont décidables ou non. Par exemple, existe-t-il un algorithme permettant de décider si un nombre p donné est premier ou non ? On sait depuis bien longtemps (au moins depuis Eratosthène et son crible) que la réponse est oui. Lorsqu'on veut être formel, on dit : l'ensemble $\{p \in \mathbb{N} \; ; \; p \text{ est premier}\}$ est récursif. Profitons-en pour donner une définition précise :

4.9 DEFINITION : *Soit* $B(x_1,x_2,\ldots,x_p)$ *une propriété portant sur les entiers* $x_1,x_2,\ldots,x_p$ *; on dit que le problème : « est-ce-que la suite* $(x_1,x_2,\ldots,x_p)$ *vérifie* B *? » est* ***décidable*** *si l'ensemble des suites* $(x_1,x_2,\ldots,x_p)$ *telles que* $B(x_1,x_2,\ldots,x_p)$ *soit vrai est récursif.*

On ne se restreint pas aux propriétés portant sur les entiers ; comme dans le cas des machines de Turing, on peut utiliser des codages par des entiers. Le chapitre suivant est riche en exemples de ce type. Le mot décidable utilisé ici évoque la notion intuitive de décidabilité, c'est-à-dire la décidabilité par un moyen mécanique ; il est totalement justifié si on est convaincu de la validité de la thèse de Church.

Le théorème smn

4.10 Sous ce nom barbare se cache un théorème extrêmement important dont la signification est la suivante : considérons la fonction partielle $f \in \mathfrak{F}^*_{n+m}$ d'indice i et fixons les n premières variables ; donnons-leur par exemple les valeurs $a_1,a_2,\ldots,a_n$. Il reste une fonction partielle $g \in \mathfrak{F}^*_m$ donnée par :

$$g = \lambda y_1 y_2 \ldots y_m . f(a_1,a_2,\ldots,a_n,y_1,y_2,\ldots,y_m),$$

qui est manifestement récursive ; et bien, un indice pour cette fonction g peut être calculé de façon effective à partir de i et de $a_1,a_2,\ldots,a_n$.

THEOREME SMN : *Pour chaque couple d'entiers* m *et* n, *il existe une fonction récursive primitive* s^m_n *à* $n+1$ *variables telle que, pour tous* i, x_1, x_2, ..., x_n, y_1, y_2, ..., y_m, *on ait :*

$$\varphi^{n+m}(i,x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_m) = \varphi^m(s^m_n(i,x_1,x_2,\ldots,x_n),y_1,y_2,\ldots,y_m).$$

⊖ La valeur de $s_n^m(i,x_1,x_2,\dots,x_n)$ est définie par cas suivant que $i \in I_{n+m}$ (qui est l'ensemble des indices des machines de Turing ayant au moins $n + m + 1$ bandes et qui, rappelons-le, est récursif primitif) ou non. Soit i_0 un entier qui n'est pas l'indice d'une machine de Turing (0, par exemple, convient parfaitement).

• Si $i \notin I_{n+m}$, on pose $s_n^m(i,x_1,x_2,\dots,x_n) = i_0$; alors ni $\varphi^{n+m}(i,x_1,x_2,\dots,x_n,y_1,y_2,\dots,y_m)$ ni $\varphi^m(s_n^m(i,x_1,x_2,\dots,x_n),y_1,y_2,\dots,y_m)$ ne sont définis.

• Le cas intéressant est celui où $i \in I_{m+n}$. Soit $\mathcal{M}$ la machine d'indice i et fixons des entiers $a_1,a_2,\dots,a_n$; il n'est pas difficile d'imaginer une machine $\mathcal{M}'$, ayant le même nombre de bandes que $\mathcal{M}$, et qui fonctionne comme suit :

1) tout d'abord elle écrit a_1 bâtons sur la bande numéro $m + 2$, a_2 bâtons sur la bande numéro $m + 3$, etc., et a_n bâtons sur la bande numéro $m + n + 1$;

2) ensuite elle travaille comme le ferait $\mathcal{M}$, à ceci près que les rôles des différentes bandes sont permutés : la bande numéro $m + 2$ (où est représenté a_1) doit être considérée comme la première bande, et d'une façon générale, pour k compris entre 1 et n, la bande numéro $m + k + 1$ (où a_k est représenté) doit être considérée comme la k-ème bande ; de plus, pour k compris entre 1 et m, la k-ème bande doit être considérée comme la bande numéro $n + k$; quant à la bande numéro $m + 1$, elle joue le rôle de la bande numéro $n + m + 1$ (et c'est donc sur cette bande que sera écrit le résultat) ;

3) enfin elle efface le contenu des bandes numéro $m + 2, m + 3, \dots, m + n$.

Deux faits sont maintenant à peu près clairs :

Premièrement, la description de $\mathcal{M}'$ est complètement explicite et effective à partir de celle de $\mathcal{M}$ et de la donnée de $a_1,a_2,\dots,a_n$; il serait horriblement ennuyeux, mais très facile de trouver une fonction récursive primitive à $n + 1$ variables, que l'on appellera s_n^m, telle que $s_n^m(i,a_1,a_2,\dots,a_n)$ soit l'indice de la machine $\mathcal{M}'$ lorsque $i \in I_{m+n}$.

Deuxièmement, si on fait fonctionner les machines $\mathcal{M}$ et $\mathcal{M}'$, avec comme configuration initiale :

• pour k compris entre 1 et m, le contenu de la k-ème bande de $\mathcal{M}'$ égal au contenu de la bande numéro $n + k$ de $\mathcal{M}$;

• toutes les autres bandes de $\mathcal{M}'$ blanches ;

• pour k compris entre 1 et n, a_k représenté sur la bande numéro k de $\mathcal{M}$,

alors, aux permutations des bandes près, ces deux machines vont travailler exactement de la même façon ; en particulier, l'une d'elle s'arrête si et seulement si l'autre s'arrête, et dans ce cas le contenu de la bande numéro $m + 1$ de $\mathcal{M}'$ sera égal au contenu de la bande numéro $n + m + 1$ de $\mathcal{M}$. Par conséquent, en se reportant à la définition des fonctions φ^p (3.17), on voit que, pour tous $x_1,x_2,\dots,x_n,y_1,y_2,\dots,y_m$,

$$\varphi^{n+m}(i,x_1,x_2,\dots,x_n,y_1,y_2,\dots,y_m) = \varphi^m(s_n^m(i,x_1,x_2,\dots,x_n),y_1,y_2,\dots,y_m).$$

☺

4.11 On va voir quelques applications de ce théorème :

EXEMPLE : Il existe une fonction récursive primitive $pl(i,j)$ telle que, si $f = \varphi_i^1$ et $g = \varphi_j^1$, $pl(i,j)$ est un indice pour la fonction partielle $f + g$.

⊖ Considérons la fonction partielle :

$$\lambda ijx.\varphi^1(i,x) + \varphi^1(j,x).$$

Elle est manifestement récursive, et donc il existe un entier k telle que cette fonction soit égale à φ_k^3. Or, pour tous i, j, x,

$$\varphi_k^3(i,j,x) = \varphi^3(k,i,j,x) = \varphi^1(s_2^1(k,i,j),x) = \varphi^1(i,x) + \varphi^1(j,x)$$

Il suffit donc de prendre $pl = \lambda ij.s_2^1(k,i,j)$.

⊕

On pourrait faire exactement la même chose avec la multiplication ou n'importe quelle fonction partielle récursive.

EXEMPLE : Soient n et p des entiers ; il existe une fonction récursive primitive $Comp(i_1,i_2,...,i_n,j)$ telle que : si, pour k compris entre 1 et n, $f_k \in \mathfrak{F}_p^*$ est la fonction partielle d'indice i_k, et si $g \in \mathfrak{F}_n^*$ est la fonction partielle d'indice j, alors $Comp(i_1,i_2,...,i_n,j)$ est un indice pour la fonction partielle $h = g(f_1,f_2,...,f_n)$.

⊖ La preuve est tout-à-fait analogue à la précédente. Considérons la fonction partielle :

$$\lambda i_1i_2...i_njx_1x_2...x_p.\varphi^n(j,\varphi^p(i_1,x_1,x_2,...,x_p),\varphi^p(i_2,x_1,x_2,...,x_p),...,\varphi^p(i_n,x_1,x_2,...,x_p)).$$

Elle est récursive, et donc il existe un entier k tel que cette fonction partielle soit égale à φ_k^{n+p+1}. On a alors :

$$\varphi^{n+p+1}(k,i_1,i_2,...,i_n,j,x_1,x_2,...,x_p) = \varphi^p(s_{n+1}^p(k,i_1,i_2,...,i_n,j),x_1,x_2,...,x_p) \ ,$$

et on peut prendre :

$$Comp = \lambda i_1i_2...i_nj.s_{n+1}^p(k,i_1,i_2,...,i_n,j).$$

⊕

4.12 Le **théorème de Rice** que nous allons montrer maintenant est un autre exemple d'application du théorème smn. Il permet de prouver que certains ensembles d'entiers ne sont pas récursifs.

THEOREME : *Soit $\mathfrak{X}$ un ensemble de fonctions partielles récursives à une variable, que l'on suppose non vide, et distinct de l'ensemble de toutes les fonctions partielles récursives. Alors l'ensemble $A = \{x \ ; \ \varphi_x^1 \in \mathfrak{X}\}$ n'est pas récursif.*

☹ Il est équivalent de montrer que A ou que son complémentaire n'est pas récursif ; en échangeant éventuellement ces deux ensembles et en remplaçant $\mathfrak{X}$ par son complémentaire dans l'ensemble des fonctions partielles récursives à une variable, on peut donc supposer que la fonction partielle θ_0 de domaine vide est dans $\mathfrak{X}$.

Fixons un entier b n'appartenant pas à A, et définissons la fonction partielle récursive $\psi \in \mathfrak{F}_3^*$:

$$\psi(x,y,z) = \varphi^1(b,z) + \varphi^1(x,y) - \varphi^1(x,y).$$

Posons aussi :

$$\psi_{x,y} = \lambda z.\psi(x,y,z).$$

Si $\varphi^1(x,y)$ n'est pas définie, la fonction partielle $\psi_{x,y}$ n'est jamais définie (donc est égale à θ_0), donc est dans $\mathfrak{X}$; sinon $\psi_{x,y}$ est égale à φ_b^1 et n'est pas dans $\mathfrak{X}$; donc $\psi_{x,y}$ appartient à $\mathfrak{X}$ si et seulement si $\varphi^1(x,y)$ n'est pas définie. On applique maintenant le théorème smn : il existe un entier k tel que :

$$\psi(x,y,z) = \varphi^3(k,x,y,z) = \varphi^1(s_2^1(k,x,y),z).$$

La fonction $h = \lambda xy.s_2^1(k,x,y)$ est récursive primitive, et $h(x,y)$ est un indice pour $\psi_{x,y}$.

On va se servir maintenant du fait que l'ensemble $W = \{(x,y) \; ; \; \varphi^1(x,y)$ n'est pas définie$\}$ n'est pas récursif (on a montré en 4.8. que son complémentaire ne l'est pas), et on remarque que $(x,y) \in W$ si et seulement si $h(x,y) \in A$. Cela montre que A ne saurait être récursif, sinon W le serait aussi (voir 2.10 et 1.6).

☺

REMARQUE : l'hypothèse « $\mathfrak{X}$ non vide et distinct de l'ensemble de toutes les fonctions partielles récursives » est évidemment indispensable (sinon A est égal à l'ensemble vide ou à $\mathbb{N}$ tout entier et la conclusion du théorème est fausse). Cette hypothèse a été utilisée lorsqu'on a choisi un entier b n'appartenant pas à A.

Voici quelques corollaires du théorème de Rice :

• Si $f \in \mathfrak{F}_p^*$ est une fonction partielle récursive, l'ensemble des indices de f n'est pas récursif (prendre $\mathfrak{X} = \{f\}$ dans le théorème de Rice) ; en particulier il n'est pas fini. Intuitivement, si une fonction partielle est calculable, elle est calculable par une infinité de machines. En fait on a bien plus que cela : on ne peut pas donner une description effective de toutes les machines calculant f.

• Le problème de savoir si deux machines calculent la même fonction partielle est indécidable : pour chaque entier p, l'ensemble

$$X = \{(i,j) \; ; \; \varphi_i^p = \varphi_j^p\}$$

n'est pas récursif.

En effet si cet ensemble était récursif, alors l'ensemble

$$\{i \; ; \; (i,0) \in X\} = \{i \; ; \; \varphi_i^p = \varphi_0^p\}$$

le serait aussi, et on a vu que ce n'est pas le cas.

• Aussi, par exemple, l'ensemble $\{n \; ; \varphi^1_n$ est totale$\}$ n'est pas récursif. Il suffit de prendre pour $\mathfrak{X}$ l'ensemble des fonctions totales récursives.

4.13 D'après le premier corollaire, si une fonction partielle a un indice i, elle a un indice supérieur à i. Le théorème suivant donne une version plus précise de ce fait.

THEOREME : *Pour chaque entier* p, *il existe une fonction récursive primitive* α *à deux variables telle que :*

- *pour tous* i *et* n $\varphi^p_i = \varphi^p_{\alpha(i,n)}$;
- *pour tout* i, *la fonction* $\lambda n.\alpha(i,n)$ *est strictement croissante.*

☺ Il suffit de construire une fonction récursive primitive β à une variable telle que, pour tout i : $\beta(i) > i$ et $\varphi^p_{\beta(i)} = \varphi^p_i$; α sera ensuite définie par récurrence par :

$$\alpha(i,0) = i \; ;$$
$$\alpha(i,n+1) = \beta(\alpha(i,n)).$$

Sans entrer dans les détails, nous allons expliquer comment calculer $\beta(i)$. Si i n'est pas l'indice d'une machine de Turing, on prend pour $\beta(i)$ un entier qui n'est pas non plus l'indice d'une machine de Turing et qui est supérieur à i (cela se trouve facilement). Si i est l'indice d'une machine de Turing $\mathcal{M}$, on complique de façon arbitraire la machine $\mathcal{M}$ (par exemple en ajoutant un état qui ne servira jamais). L'indice de la nouvelle machine, si on s'y prend bien, est strictement supérieur à i et est une fonction récursive primitive de i, et évidemment les deux machines fonctionnent exactement de la même façon et calculent donc la même fonction.

☺

L'exercice 26 donne une preuve de ce théorème à partir des théorèmes smn et du point fixe (voir ci-dessous).

Les théorèmes de point fixe

4.14 Ce sont des théorèmes qui sont aussi très importants et qui sont dus à S. Kleene. On les appelle quelquefois **théorèmes de la récursion** (les quelques exemples d'application qui suivront justifieront ce nom).

THEOREME DU POINT FIXE, PREMIERE VERSION : *Soient* p *un entier positif et* α *une fonction récursive (totale) à une variable ; alors il existe un entier* i *tel que*

$$\varphi_i^p = \varphi_{\alpha(i)}^p .$$

☹ Considérons la fonction partielle $\lambda y x_1 x_2 \ldots x_p . \varphi^p(\alpha(s_1^p(y,y)),x_1,x_2,\ldots,x_p)$. Elle est récursive ; elle admet donc un indice a, et on a pour tous $x_1,x_2,\ldots,x_p$ et y :

$$\varphi^{p+1}(a,y,x_1,x_2,\ldots,x_p) = \varphi^p(\alpha(s_1^p(y,y)),x_1,x_2,\ldots,x_p) = \varphi^p(s_1^p(a,y),x_1,x_2,\ldots,x_p).$$

et, en faisant $y = a$ dans les égalités précédentes et en posant $i = s_1^p(a,a)$, on obtient :

$$\varphi_i^p = \varphi_{\alpha(i)}^p$$

☺

REMARQUE : L'entier i peut être trouvé de façon récursive primitive à partir d'un indice de α : supposons que $\alpha = \varphi_j^1$. Il s'agit d'abord de calculer un indice a de la fonction partielle $\lambda y x_1 x_2 \ldots x_p . \varphi^p(\alpha(s_1^p(y,y)),x_1,x_2,\ldots,x_p)$. C'est encore une utilisation du théorème smn : soit b un indice de la fonction partielle $\lambda j y x_1 x_2 \ldots x_p . \varphi^p(\varphi^1(j,s_1^p(y,y)),x_1,x_2,\ldots,x_p)$. On a alors pour tous $x_1,x_2,\ldots,x_p$ et y :

$$\varphi^p(\alpha(s_1^p(y,y)),x_1,x_2,\ldots,x_p) = \varphi^p(\varphi^1(j,s_1^p(y,y)),x_1,x_2,\ldots,x_p) = \varphi^{p+2}(b,j,y,x_1,x_2,\ldots,x_p) =$$
$$\varphi^{p+1}(s_1^{p+1}(b,j),y,x_1,x_2,\ldots,x_p).$$

On peut donc prendre $a = s_1^{p+1}(b,j)$ et on pose encore $i = s_1^p(a,a)$. On vient donc de démontrer :

THEOREME DU POINT FIXE, DEUXIEME VERSION : *Pour chaque entier positif* p, *il existe une fonction récursive primitive* h_p *à une variable telle que, pour tout* j, *si* $\alpha = \varphi_j^1$ *est une fonction totale, alors*

$$\varphi^p_{h_p(j)} = \varphi^p_{\alpha(h_p(j))} .$$

Voyons une dernière version du théorème du point fixe :

THEOREME DU POINT FIXE, TROISIEME VERSION : *Soient* $n > 0$ *et* p *des entiers et* α *une fonction totale récursive à* $p + 1$ *variables. Alors il existe une fonction récursive primitive* h *à* p *variables telle que, pour tous* $x_1,x_2,\ldots,x_p$, *on ait :*

$$\varphi^n_{\alpha(x_1,x_2,\ldots,x_p,h(x_1,x_2,\ldots,x_p))} = \varphi^n_{h(x_1,x_2,\ldots,x_p)} .$$

⊖ Soit a un indice pour la fonction partielle

$$\lambda z x_1 x_2 \ldots x_p y_1 y_2 \ldots y_n . \varphi^n(\alpha(x_1,x_2,\ldots,x_p,s^n_{p+1}(z,z,x_1,x_2,\ldots,x_p)),y_1,y_2,\ldots,y_n).$$

On a donc, pour tous $x_1,x_2,\ldots,x_p,y_1,y_2,\ldots,y_n$ et z :

$$\varphi^n(\alpha(x_1,x_2,\ldots,x_p,s^n_{p+1}(z,z,x_1,x_2,\ldots,x_p)),y_1,y_2,\ldots,y_n) =$$
$$\varphi^{n+p+1}(a,z,x_1,x_2,\ldots,x_p,y_1,y_2,\ldots,y_n) = \varphi^n(s^n_{p+1}(a,z,x_1,x_2,\ldots,x_p),y_1,y_2,\ldots,y_n).$$

En faisant $z = a$, on obtient :

$$\varphi^n(\alpha(x_1,x_2,\ldots,x_p,s^n_{p+1}(a,a,x_1,x_2,\ldots,x_p)),y_1,y_2,\ldots,y_n) = \varphi^n(s^n_{p+1}(a,a,x_1,x_2,\ldots,x_p),y_1,y_2,\ldots,y_n)$$

et on peut prendre $h(x_1,x_2,\ldots,x_p) = s^n_{p+1}(a,a,x_1,x_2,\ldots,x_p)$.

⊕

REMARQUE : Là aussi, on pourrait calculer un indice pour h de façon récursive primitive à partir d'un indice de α.

4.15 On va donner des exemples d'application de ces théorèmes ; ces exemples montrent comment les théorèmes du point fixe permettent de généraliser les définitions par récurrence.

EXEMPLE : Considérons la fonction partielle f à deux variables (ce serait exactement la même chose si on prenait une fonction partielle à $n+1$ variables) définie par récurrence par :

$$f(x,0) = g(x),$$
$$f(x,y+1) = h(x,y,f(x,y)),$$

où g et h sont des fonctions partielles récursives. Alors, on peut calculer un indice pour f de façon récursive primitive à partir d'un indice pour g et d'un indice pour h.

⊖ Considérons en effet l'application de $\mathfrak{F}_2^*$ dans $\mathfrak{F}_2^*$ qui à ψ fait correspondre la fonction partielle ψ^* définie de la façon suivante :

- $\psi^*(x,y) = g(x)$ si $y = 0$,
- $\psi^*(x,y) = h(x,y-1,\psi(x,y-1))$ sinon.

On remarque d'abord que f est le seul point fixe de cette application : c'est la seule fonction partielle qui satisfasse $f = f^*$. D'autre part, si ψ est récursive, il en est de même de ψ^*, et, de plus, on peut calculer un indice pour ψ^* à partir des indices respectifs i_1,i_2 et i_3 de g, h et ψ. Il s'agit là d'une application du théorème smn comme on en a déjà vues : considérons la fonction partielle récursive $k(i_1,i_2,i_3,x,y)$ définie par :

$$k(i_1,i_2,i_3,x,y) = \varphi^1(i_1,x) \text{ si } y = 0,$$
$$k(i_1,i_2,i_3,x,y) = \varphi^3(i_2,x,y-1,\varphi^2(i_3,x,y-1)) \text{ sinon.}$$

La fonction partielle ψ^* est précisément égale à $\lambda xy.k(i_1,i_2,i_3,x,y)$. Si a est un indice de k, on a :

$$k(i_1,i_2,i_3,x,y) = \varphi^5(a,i_1,i_2,i_3,x,y) = \varphi^2(s^2_3(a,i_1,i_2,i_3),x,y).$$

Posons $\alpha(i_1,i_2,i_3) = s^2_3(a,i_1,i_2,i_3)$; α est une fonction récursive primitive qui calcule un

indice pour ψ^* comme promis : $(\varphi^2_{i_3})^* = \varphi^2_{\alpha(i_1,i_2,i_3)}$. Appliquons maintenant la troisième version du théorème du point fixe : il existe une fonction récursive primitive $j \in \mathfrak{F}_2$ telle que, pour tous z,t, $\varphi^2_{\alpha(z,t,j(z,t))} = \varphi^2_{j(z,t)}$, ce qui montre que $(\varphi^2_{j(i_1,i_2)})^* = \varphi^2_{j(i_1,i_2)}$ et donc, d'après la remarque initiale, que $\varphi^2_{j(i_1,i_2)} = f$.

☺

4.16 EXEMPLE : Pour couronner ce chapitre, on va montrer que la fonction d'Ackermann est récursive. On aurait pu le faire plus tôt en construisant une machine de Turing qui la calcule, mais la preuve qui suit est bien plus élégante. C'est certainement un procédé de récurrence qui a été utilisé pour définir cette fonction, mais ce procédé n'entre pas dans le cadre du schéma de définition par récurrence décrit tout au début de ce chapitre. On va voir comment les théorèmes du point fixe permettent de montrer que les fonctions définies par ce procédé sont encore récursives.

Considérons l'application de $\mathfrak{F}_2^*$ dans $\mathfrak{F}_2^*$ qui à ψ fait correspondre la fonction partielle ψ^* définie par :

$\psi^*(y,x) = 2^x$ si $y = 0$;
$\psi^*(y,x) = 1$ si $x = 0$;
$\psi^*(y,x) = \psi(y - 1, \psi(y,x - 1))$ dans les autres cas.

En se reportant à la définition de la fonction d'Ackermann en 2.1, on se rend compte que celle-ci est le seul point fixe de cette transformation. Donc, si on démontre qu'il existe une fonction partielle récursive ζ telle que $\zeta^* = \zeta$, alors ζ sera nécessairement égale à la fonction d'Ackermann, qui sera donc récursive. On raisonne comme plus haut : si ψ est une fonction partielle récursive, il en est de même de ψ^*, et voyons comment calculer, de façon récursive primitive, un indice pour ψ^* à partir d'un indice de ψ.

Définissons $\theta \in \mathfrak{F}_3^*$ par :

- $\theta(i,y,x) = 2^x$ si $y = 0$;
- $\theta(i,y,x) = 1$ si $x = 0$;
- $\theta(i,y,x) = \varphi^2(i,y - 1, \varphi^2(i,y,x - 1))$ sinon.

La fonction partielle récursive θ a été définie de telle sorte que $\lambda xy.\theta(i,x,y)$ soit égale à ψ^* si $\psi = \varphi^2_i$. Soit a un indice de θ. Alors :

$$\theta(i,x,y) = \varphi^3(a,i,x,y) = \varphi^2(s^2_1(a,i),x,y).$$

Posons $\alpha(i) = s^2_1(a,i)$; α est une fonction récursive primitive qui donne un indice de ψ^* à partir d'un indice de ψ. Appliquons alors le théorème du point fixe première version : il existe un entier j tel que $\varphi^2_j = \varphi^2_{\alpha(j)}$, et donc tel que $(\varphi^2_j)^* = \varphi^2_j$. La fonction d'Ackermann est récursive.

☺

EXERCICES

1. Montrer que tout sous-ensemble fini de $\mathbb{N}$ est récursif primitif.

2. Montrer que la fonction f définie par :

- $f(0) = f(1) = 1$
- $f(n + 2) = f(n) + f(n + 1)$

est récursive primitive.
(Cette suite est appelée **suite de Fibonacci**.)

3. Dans cet exercice, on pose $\mathscr{S}^* = \bigcup_{p>0} \mathbb{N}^p$. On définit l'application α de $\mathscr{S}^*$ dans $\mathbb{N}$: si σ est une suite d'entiers de longueur p, alors $\alpha(\sigma) = \alpha_2(p, \alpha_p(\sigma))$.

a) Montrer que α est une fonction injective dont l'image est un ensemble récursif primitif.

b) Montrer qu'il existe une fonction récursive primitive g telle que, si $\sigma = (a_1, a_2, \ldots, a_n)$, et si $b = \sup(n, a_1, a_2, \ldots, a_n)$, alors $\alpha(\sigma) \leqslant g(b)$.

c) Montrer que la fonction φ définie par :

- $\varphi(p,i,x) = \beta_p^i(x)$ si $1 \leqslant i \leqslant p$
- $\varphi(p,i,x) = 0$ sinon

est récursive primitive.

d) On définit maintenant un autre codage : soit γ la fonction qui, à toute suite $(a_0, a_1, \ldots, a_p)$ de $\mathscr{S}^*$, fait correspondre l'entier :

$$\gamma((a_0, a_1, \ldots, a_p)) = \pi(0)^{a_0+1} \cdot \pi(1)^{a_1+1} \cdot \ldots \cdot \pi(p)^{a_p+1} .$$

Montrer que γ est une application injective et que son image est un ensemble récursif primitif.

e) Montrer que l'on peut passer d'un codage à l'autre de façon récursive primitive ; plus précisément, il existe deux fonctions récursives primitives f et h à une variable telles que :

i) pour tout x dans l'image de α, $f(x) = \gamma(\sigma)$ où σ est la suite non vide telle que $\alpha(\sigma) = x$;

ii) pour tout x appartenant à l'image de γ, $h(x) = \alpha(\sigma)$ où σ est la suite non vide telle que $\gamma(\sigma) = x$.

4. Montrer que la fonction qui à n fait correspondre la n-ème décimale du nombre e, base du logarithme népérien, est récursive primitive.

5. a) On fixe un entier p non nul. Montrer que l'ensemble

$$E = \{ (a_0,a_1,\ldots,a_p) \in \mathbb{N}^p \text{ ; le polynôme } a_0 + a_1X + \cdots + a_pX^p \text{ a un zéro dans } \mathbb{Z} \}$$

est récursif primitif.

b) Même question en remplaçant $\mathbb{Z}$ par $\mathbb{Q}$.

c) Montrer que l'ensemble

$$F = \{ \Omega(\sigma) \text{ ; } p \text{ est un entier, } \sigma = (a_0,a_1,\ldots,a_p) \text{ et le polynôme } a_0 + a_1X + \cdots + a_pX^p \text{ a un zéro dans } \mathbb{Z} \}$$

est récursif primitif (Ω est le codage défini en 1.12).

6. Soient L un langage comportant uniquement le symbole de prédicat binaire R et F une formule close de L. Le **spectre** de F, que l'on notera $Sp(F)$, est par définition l'ensemble

$$\{ n \in \mathbb{N} \text{ ; } F \text{ a un modèle de cardinalité } n \}.$$

(Voir l'exercice 10 du chapitre 3.)
Montrer que $Sp(F)$ est un ensemble récursif primitif.

7. Pour chacune des fonctions suivantes, construire une machine de Turing qui la calcule :

a) $\lambda x.x^2$; b) $\lambda xy.xy$; c) $\lambda x.x \dot{-} 1$; d) $\lambda xy.x \dot{-} y$.

8. Construire une machine de Turing qui s'arrête si et seulement si l'entier que l'on a rentré sur la première bande à l'instant initial est pair.

9. a) Montrer que, si une fonction partielle $f \in \mathfrak{F}_1^*$ est T-calculable, elle est calculable par une machine de Turing ayant exactement 3 bandes.

b) On considère l'ensemble $\mathfrak{M}_n$ des machines ayant 3 bandes et n états. On fait fonctionner ces machines à partir d'une configuration initiale où toutes les bandes sont blanches. Si la machine $\mathscr{M}$ s'arrête, on appelle $\sigma(\mathscr{M})$ le nombre de bâtons écrits sur la seconde bande au moment de l'arrêt ; sinon on pose $\sigma(\mathscr{M}) = 0$. Montrer que l'ensemble

$$\{ \sigma(\mathscr{M}) \text{ ; } \mathscr{M} \in \mathfrak{M}_n \}$$

est borné. On notera $\Sigma(n)$ la borne supérieure de cet ensemble.

c) Soit f une fonction partielle à une variable calculable par une machine $\mathscr{M}$ de $\mathfrak{M}_n$. Pour chaque entier p, construire une machine $\mathscr{N}_p$ à trois bandes qui, si on la fait fonctionner à partir d'une configuration initiale où toutes les bandes sont blanches, commence à écrire p bâtons sur la première bande, puis ramène sa tête en début de bande, et enfin fonctionne comme le ferait $\mathscr{M}$.

Préciser le nombre d'états de $\mathscr{N}_p$.

d) Montrer que la fonction Σ n'est pas T-calculable.

10. Soit $f \in \mathfrak{F}_1$; Montrer que f est récursive si et seulement si son graphe

$$G = \{ (x,y) \in \mathbb{N}^2 \,;\, y = f(x) \}$$

est récursif.

11. Le but de cet exercice est de donner une preuve directe du fait que la fonction d'Ackermann est récursive.

On définit sur $\mathbb{N}^3$ la relation binaire $\ll$ par : $(a,b,c) \ll (a',b',c')$ si et seulement si :

$\sup(a,b,c) < \sup(a',b',c')$

ou $\sup(a,b,c) = \sup(a',b',c')$ et $a < a'$

ou $\sup(a,b,c) = \sup(a',b',c')$ et $a = a'$ et $b < b'$

ou $\sup(a,b,c) = \sup(a',b',c')$ et $a = a'$ et $b = b'$ et $c \leqslant c'$.

a) Montrer que $\ll$ est une relation d'ordre total.

Si α et β appartiennent à $\mathbb{N}^3$, on dira que α est **inférieur ou égal** (respectivement : **supérieur ou égal**) à β si $\alpha \ll \beta$ (respectivement $\beta \ll \alpha$). On dira que α est **strictement inférieur** (respectivement : **strictement supérieur**) à β si, de plus, $\alpha \neq \beta$.

Montrer que, pour tout $(a,b,c) \in \mathbb{N}^3$, l'ensemble $\{ (x,y,z) \in \mathbb{N}^3 \,;\, (x,y,z) \ll (a,b,c) \}$ a au plus $(\sup(a,b,c) + 1)^3$ éléments. Montrer que tout élément $(a,b,c) \in \mathbb{N}^3$ possède un successeur immédiat (c'est-à-dire un élément qui est strictement supérieur à (a,b,c) et qui est inférieur ou égal à tous les éléments strictement supérieurs à (a,b,c)). On explicitera ce successeur immédiat.

b) Montrer qu'il existe trois fonctions de $\mathbb{N}$ dans $\mathbb{N}$, récursives primitives, γ_1, γ_2, γ_3, telles que :

1°) la fonction Γ de $\mathbb{N}$ dans $\mathbb{N}^3$ définie par $\Gamma(n) = (\gamma_1(n), \gamma_2(n), \gamma_3(n))$ est une bijection ;

2°) pour tous entiers n et m, $n \leqslant m$ si et seulement si $\Gamma(n) \ll \Gamma(m)$.

c) Soit H le sous-ensemble de $\mathbb{N}$ défini récursivement par la condition : $n \in H$ si et seulement si :

- $\gamma_2(n) = 0$ et $\gamma_1(n) = 2^{\gamma_3(n)}$;

ou
- $\gamma_3(n) = 0$ et $\gamma_1(n) = 1$;

ou
- $\gamma_2(n) \neq 0$ et $\gamma_3(n) \neq 0$ et il existe des entiers p et q, strictement inférieurs à n, tels que $p \in H$, $q \in H$, $\gamma_2(p) = \gamma_2(n)$, $\gamma_3(p) = \gamma_3(n) - 1$, $\gamma_2(q) = \gamma_2(n) - 1$, $\gamma_3(q) = \gamma_1(p)$ et $\gamma_1(n) = \gamma_1(q)$.

Montrer que H est récursif primitif.

On appelle, comme dans le cours, ξ la fonction d'Ackermann. Montrer que, pour tout entier n, $n \in H$ si et seulement si $\gamma_1(n) = \xi(\gamma_2(n), \gamma_3(n))$.

d) Montrer que le graphe G de la fonction d'Ackermann :

$$G = \{ (y,x,z) \,;\, z = \xi(y,x) \},$$

est récursif primitif. Montrer que la fonction d'Ackermann est récursive.

12. Montrer que l'image d'une fonction à une variable récursive et croissante est un ensemble récursif. Réciproquement, montrer que tout ensemble récursif infini est l'image d'une fonction récursive strictement croissante.

13. Soit $f \in \mathfrak{F}_1$ une fonction récursive et on suppose que son image est infinie. Montrer qu'il existe une fonction $g \in \mathfrak{F}_1$, récursive, injective, telle que $\mathrm{Im}(f) = \mathrm{Im}(g)$. En déduire qu'il existe une fonction récursive injective dont l'image n'est pas récursive.

14. Montrer que tout ensemble récursivement énumérable infini contient un ensemble récursif infini.

15. Soient α une fonction récursive injective. On pose :

$A = \mathrm{Im}\,\alpha$;

$B = \{x$; il existe $y > x$ tel que $\alpha(y) < \alpha(x)\}$.

a) Montrer que B est récursivement énumérable et que son complémentaire est infini.

b) On suppose qu'il existe un sous-ensemble C de $\mathbb{N}$, récursivement énumérable, infini et disjoint de B. Montrer que A est récursif.

c) Montrer qu'il existe un ensemble récursivement énumérable qui, premièrement, rencontre tous les ensembles récursivement énumérables infinis, et, deuxièmement, a un complémentaire infini.

16. a) Montrer que l'ensemble des bijections récursives de $\mathbb{N}$ dans $\mathbb{N}$ est un sous-groupe du groupe des permutations de $\mathbb{N}$.

La suite du problème est consacrée au fait que cette assertion devient fausse si on remplace récursive par récursive primitive.

b) Soient φ une fonction (totale) à une variable, récursive mais non récursive primitive, et e l'indice d'une machine $\mathcal{M}$ qui calcule φ. On considère la fonction T qui à x fait correspondre le temps de calcul de $\varphi(x)$ par $\mathcal{M}$ (plus précisément : $T(x) = \mu t\ ((e,t,x) \in B^1)$).

Montrer que, si f est une fonction telle que, pour tout $x \in \mathbb{N}$, $f(x) \geqslant T(x)$, alors f n'est pas récursive primitive ; Montrer que le graphe G de T est récursif primitif.

c) On pose :

$$g(x) = \sup\{T(y)\ ;\ y \leqslant x\} + 2x.$$

Montrer que g est une fonction récursive, strictement croissante, et qu'elle n'est pas récursive primitive. Montrer que le graphe G_1 et que l'image I de g sont des ensembles récursifs primitifs.

d) Montrer qu'il existe une unique fonction g' récursive primitive strictement croissante dont l'image soit le complémentaire de I.

e) On définit la fonction h par :

- $h(2x) = g(x)$
- $h(2x + 1) = g'(x)$

où g et g' sont les fonctions définies aux questions c) et d). Montrer que h est une fonction bijective, récursive, non récursive primitive. Montrer que sa réciproque h^{-1} est récursive primitive.

17. Exhiber un ensemble récursif $A \subseteq \mathbb{N}^2$ tel que l'ensemble

$$B = \{x \,;\, \text{pour tout } y \in \mathbb{N},\ (x,y) \in A\}$$

ne soit pas récursivement énumérable.

18. Montrer qu'il existe une fonction récursive primitive α à une variable possédant la propriété suivante : pour tout entier x, si φ^1_x est une bijection de $\mathbb{N}$ dans $\mathbb{N}$, alors $\alpha(x)$ est un indice pour la bijection réciproque.

19. Soient g et α dans $\mathfrak{F}^*_1$ et $h \in \mathfrak{F}^*_3$ des fonctions partielles récursives. Montrer qu'il existe une et une seule fonction $f \in \mathfrak{F}^*_2$ telle que pour tous x, y :

$$f(0,y) = g(y)$$
$$f(x + 1,y) = h(f(x,\alpha(y)),y,x),$$

et que f est partielle récursive.

20. Soient $A \subseteq \mathbb{N}$ un ensemble récursivement énumérable qui n'est pas récursif, f une fonction partielle récursive de domaine A et i l'indice d'une machine de Turing calculant f. Montrer que la fonction $\lambda x.T^1(i,x)$ (où T^1 est la fonction définie en 3.18 et qui représente le temps nécessaire au calcul de $f(x)$) ne peut pas être prolongée en une fonction récursive totale.

21. Le but de cet exercice est de montrer le fait suivant:

(*) *Il existe une fonction (totale) récursive* $\psi(x,y)$ *telle que, si on pose* $\psi_x = \lambda y.\psi(x,y)$, *alors l'ensemble*

$$\{\psi_x \,;\, x \in \mathbb{N}\}$$

est exactement l'ensemble de toutes les fonctions récursives primitives à une variable.

a) Montrer que, si $f \in \mathfrak{F}_p$, les deux conditions suivantes sont équivalentes :

i) f est récursive primitive ;

ii) il existe un indice i et une fonction $g \in \mathfrak{F}_p$ récursive primitive tels que la machine d'indice i calcule f et que le temps de calcul $T(i,x_1,x_2,\dots,x_p)$ soit inférieur ou égal à $g(x_1,x_2,\dots,x_p)$.

b) On va utiliser la fonction d'Ackermann ξ et les fonctions $\xi_n = \lambda x.\xi(n,x)$. Montrer que si f est une fonction à une variable qui est récursive primitive, il existe deux entiers n et A tels que, pour tout x, on ait :

$$f(x) \leqslant \sup(A, \xi_n(x)).$$

c) On définit la fonction g à quatre variables de la façon suivante :

$$g(i,A,n,x) = \mu y \leqslant \sup(A,\xi(n,x))\ (\exists t \leqslant \sup(A,\xi(n,x))\ (i,t,x,y) \in C^1)$$

(on rappelle que $(i,t,x,y) \in C^1$ signifie que la machine d'indice i fonctionnant avec x sur sa première bande au départ a terminé son calcul à l'intant t et que le résultat est y). Montrer que, pour tous i, A et n la fonction $\lambda x.g(i,A,n,x)$ est récursive primitive et que, réciproquement, pour toute fonction f récursive primitive à une variable, il existe des entiers i, A et n tels que $f = \lambda x.g(i,A,n,x)$.

d) En déduire le théorème cherché.

e) Montrer qu'il existe un ensemble récursif qui n'est pas récursif primitif.

22. Soit $\mathcal{F}$ un ensemble de fonctions partielles récursives à une variable. On dira que $\mathcal{F}$ est **récursivement énuméré** s'il existe une fonction F partielle récursive à deux variables telle que, si on pose $F_x = \lambda y.F(x,y)$, alors

$$\mathcal{F} = \{F_x\ ;\ x \in \mathbb{N}\}.$$

L'exercice 21 montre donc que l'ensemble des fonctions récursives primitives est récursivement énuméré.

a) Montrer que l'ensemble des fonctions totales récursives n'est pas récursivement énuméré.

b) Montrer que l'ensemble des fonctions récursives primitives strictement croissantes est récursivement énuméré.

c) Montrer que l'ensemble des fonctions récursives primitives injectives est récursivement énuméré.

d) Soit $F \in \mathfrak{F}_2$ une fonction récursive et on suppose que, pour tout $x \in \mathbb{N}$, l'ensemble

$$A_x = \{F(x,y)\ ;\ y \in \mathbb{N}\}$$

est infini. Montrer qu'il existe un ensemble B, récursif et infini, qui n'est égal à aucun des A_x. En déduire que l'ensemble des fonctions récursives strictement croissantes n'est pas récursivement énuméré, pas plus que l'ensemble des fonctions récursives injectives.

23. Soient A et B deux sous-ensembles de $\mathbb{N}$; on dit que A **est réductible à** B et on écrira $A \leqslant B$ s'il existe une fonction récursive (totale) f telle que :

$$x \in A \text{ si et seulement si } f(x) \in B.$$

a) Montrer que la relation $\leqslant$ est réflexive et transitive.

b) On suppose que A est réductible à B ; montrer que, si B est récursivement énumérable, alors A est récursivement énumérable ; montrer que, si B est récursif, alors A l'est aussi.

On pose :

$X = \{ x \,;\, \varphi^1(x,x) \text{ est défini} \}$;

$Y = \{ \alpha_2(x,y) \,;\, \varphi^1(x,y) \text{ est défini} \}$.

c) Montrer que, si $A \subseteq \mathbb{N}$, A est récursivement énumérable si et seulement si $A \leqslant Y$.

d) Soient A et B deux sous-ensembles de $\mathbb{N}$; on définit l'ensemble C par :

$$C = \{2n \,;\, n \in A\} \cup \{2n+1 \,;\, n \in B\}.$$

Montrer que A et B sont réductibles à C et que, si D est un sous-ensemble de $\mathbb{N}$ tel que A et B soient réductibles à D, alors C est réductible à D.

e) On dira que $A \subseteq \mathbb{N}$ est autodual si $A \leqslant \mathbb{N} - A$. Montrer que pour tout $B \subseteq \mathbb{N}$, il existe $C \subseteq \mathbb{N}$, autodual et tel que $B \leqslant C$.

f) Soit $\mathcal{F}$ un ensemble de fonctions partielles récursives à une variable qui n'est ni vide ni égal à l'ensemble des fonctions partielles récursives à une variable ; on pose :

$$A = \{x \,;\, \varphi^1_x \in \mathcal{F}\}.$$

i) Montrer que, si $\mathcal{F}$ contient la fonction partielle de domaine vide, alors $X \leqslant \mathbb{N} - A$.

ii) Montrer que dans le cas contraire $X \leqslant A$.

iii) Montrer que A n'est pas autodual.

g) Montrer que $Y \leqslant X$.

24. Le but de cet exercice est de montrer que les précautions que l'on a prises lorsqu'on a défini le schéma μ non borné (2.9) sont nécessaires.

Montrer que la fonction partielle $\psi(x,y)$, égale à $\varphi^1(x,y) - \varphi^1(x,y)$ si $y = 0$ et à 0 sinon, est partielle récursive.

On définit la fonction g par : $g(x)$ est le plus petit entier y tel que $\psi(x,y) = 0$. Montrer que g est une fonction totale qui n'est pas récursive.

25. On considère les ensembles suivants :

$A = \{x \,;\, \varphi^1_x(0) \text{ est défini}\}$;

$B = \{x \,;\, \varphi^1_x \text{ est une fonction totale}\}$.

a) Montrer que le complémentaire de A n'est pas récursivement énumérable.

b) Montrer qu'il existe une fonction $\alpha \in \mathfrak{F}_1$ récursive primitive telle que, pour tout entier i, $i \in A$ si et seulement si $\alpha(i) \in B$. Montrer que le complémentaire de B n'est pas récursivement énumérable.

c) On définit la fonction partielle $F(x,y)$ comme suit :

$F(x,y) = 1$ si, pour tout $z < y$, $\neg B^1(e,z,x)$;

$F(x,y)$ n'est pas définie sinon,

où B^1 est le prédicat défini en 3.18. et e est un indice d'une fonction partielle de domaine A.

Montrer que la fonction partielle $\lambda y.F(x,y)$ est totale si et seulement si $x \notin A$. En déduire que B n'est pas récursivement énumérable.

d) En généralisant les points b) et c), montrer la proposition suivante :

PROPOSITION : *Soit* f *une fonction partielle récursive à une variable de domaine infini. Alors, ni l'ensemble* $\{x ; \varphi^1_x = f\}$, *ni son complémentaire ne sont récursivement énumérables.*

26. On va donner dans cet exercice une autre preuve du fait qu'il existe une fonction récursive primitive β à une variable telle que, pour tout i,

$$\varphi^1_i = \varphi^1_{\beta(i)} \text{ et } \beta(i) > i.$$

(cf. théorème 4.13). Cette preuve n'utilise que les théorèmes du point fixe (et ne fait plus appel aux machines de Turing).

a) Montrer qu'il existe une fonction δ récursive primitive telle que, pour tout n, $\varphi^1_{\delta(n)}$ est la fonction constante égale à n.

b) On définit la fonction $\gamma(n,t,z)$ par :

$\gamma(n,t,z) = \delta(n)$ si $z \leqslant t$;

$\gamma(n,t,z) = t$ sinon.

En appliquant le théorème de point fixe troisième version (4.14) à cette fonction, montrer qu'il existe une fonction récursive primitive $h(n,t)$ telle que :

$\varphi^1_{h(n,t)} = \varphi^1_{\delta(n)}$ si $h(n,t) \leqslant t$

$\varphi^1_{h(n,t)} = \varphi^1_t$ sinon.

c) Montrer que, pour tout t, l'ensemble

$$A_t = \{n ; h(n,t) \leqslant t\}$$

a, au plus, $t + 1$ éléments. En déduire l'existence de la fonction β cherchée.

27. Dans la construction des fonctions φ^p on a fait un certain nombre de codages, et pour cela on a dû faire des choix complètement arbitraires. On s'intéresse ici à la question de savoir quelles sortes de fonctions on aurait obtenues à la place des φ^p si ces choix avaient été différents. La seule chose que l'on suppose, c'est que ces choix soient suffisamment raisonnables pour nous permettre de démontrer les théorèmes d'énumération et de point fixe.

Soit $\Psi = (\psi^p \; ; \; p \geqslant 1)$ une famille de fonctions partielles récursives telles que, pour chaque p, $\psi^p \in \mathfrak{F}^*_{p+1}$. On pose $\psi^p_x = \lambda y_1 y_2 \ldots y_p . \psi^p(x, y_1, y_2, \ldots y_p)$. On considère les conditions suivantes sur la famille Ψ :

• (énu) Pour chaque $p > 0$, l'ensemble $\{ \psi^p_i \; ; \; i \in \mathbb{N} \}$ est égal à l'ensemble de toutes les fonctions partielles récursives à p variables.

• (smn) Pour chaque couple d'entiers m et n, il existe une fonction totale récursive σ^m_n à $n + 1$ variables, telle que, pour tous $i, x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m$, on ait :

$$\psi^{n+m}(i, x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = \psi^m(\sigma^m_n(i, x_1, x_2, \ldots, x_n), y_1, y_2, \ldots, y_m).$$

a) Soit θ une fonction partielle récursive à deux variables. Pour chaque entier x, on pose $\theta_x = \lambda y . \theta(x, y)$. Montrer que les deux conditions suivantes sont équivalentes :

i) il existe une famille $\Psi = (\psi^p \; ; \; p \geqslant 1)$ vérifiant les conditions (énu) et (smn) et telle que $\psi^1 = \theta$;

ii) il existe une fonction récursive β telle que pour tout x, $\varphi^1_x = \theta_{\beta(x)}$.

b) On suppose que la famille Ψ satisfait encore les conditions (énu) et (smn). Montrer que les théorèmes du point fixe sont vrais pour la famille Ψ.

c) On suppose que la fonction θ satisfait les conditions *i)* ou *ii)* du a). Montrer qu'il existe deux fonctions récursives et injectives α et β telles que, pour tout x,

$$\varphi^1_x = \theta_{\beta(x)} \quad \text{et} \quad \theta_x = \varphi^1_{\alpha(x)}.$$

d) (difficile) Avec les mêmes hypothèses, montrer qu'il existe une fonction ε, récursive, totale et bijective, telle que, pour tout x, $\varphi^1_x = \theta_{\varepsilon(x)}$.

Chapitre 6

Formalisation de l'arithmétique Théorèmes de Gödel

La branche des mathématiques dont il est le plus naturel d'envisager la formalisation est certainement l'arithmétique. C'est à quoi est employé ce chapitre.

Dans la première section, on fixe le langage de l'arithmétique et on en donne l'ensemble des axiomes, habituellement appelés axiomes de Peano, que l'on notera $\mathscr{P}$. Ces axiomes ont pour but, pour les uns (de A_1 à A_7) de forcer l'addition et la multiplication à se conduire correctement, et pour les autres (le schéma d'axiomes SI) de permettre les fameuses démonstrations par récurrence. En apparence, ce sont des axiomes très simples, et on peut même se demander s'ils ne sont pas trop simples. Aussi la question qui se pose immédiatement est de savoir si on n'a rien oublié de ce que les mathématiciens emploient couramment. La réponse est non, mais on n'essaiera pas d'en convaincre le lecteur. On se contentera de tirer quelques conséquences extrêmement simples des axiomes, par exemple la commutativité et l'associativité de la multiplication. Rien n'empêche le lecteur de démontrer à partir des seuls axiomes de Peano des théorèmes comme ceux de Gauss ou de Bezout. Même des théorèmes beaucoup plus difficiles, comme ceux qui concernent la répartition des nombres premiers par exemple, non seulement peuvent s'exprimer sous forme d'une formule du premier ordre, mais aussi se démontrer à partir de ces axiomes.

Il y a alors deux questions qui se posent naturellement. La première concerne la complétude de $\mathscr{P}$: est-il vrai que toute formule close du langage de l'arithmétique est soit démontrée, soit réfutée (c'est-à-dire que sa négation est démontrée) dans $\mathscr{P}$? La seconde sa décidabilité : existe-t-il un algorithme permettant de décider si une formule close du langage de l'arithmétique est démontrable à partir de $\mathscr{P}$? La réponse à ces deux questions est négative et la fin du chapitre est consacrée à la preuve de ce fait, avec les célèbres théorèmes de Gödel.

La seconde question exige que l'on code les formules par des entiers. Ce travail ingrat est fait dans la troisième section ; dans la seconde section, on travaille dans l'autre sens. On montre que les fonctions récursives peuvent être représentées, dans un sens très fort, par des formules du premier ordre. Pour répondre aux questions que l'on s'est posées, on utilisera un argument « diagonal », du type de celui dont on s'est servi au chapitre précédent pour montrer qu'il y a des ensembles récursivement énumérables qui ne sont pas récursifs. Pour la réponse à la seconde question, cet argument rejoint le fameux paradoxe d'Epiménides le Crétois qui prétendait que tous les Crétois étaient menteurs (voir l'exercice 15). Dans notre cas, cela revient à construire une formule qui affirme qu'elle est elle-même non démontrable. On verra que cette formule est vraie dans $\mathbb{N}$, non démontrable dans $\mathscr{P}$, et qu'elle est équivalente (modulo $\mathscr{P}$) à une formule exprimant que $\mathscr{P}$ est une théorie cohérente.

Dans ce chapitre, nous manipulerons en même temps l'ensemble $\mathbb{N}$ des « vrais entiers » et des modèles des axiomes de Peano. Comme nous l'avons signalé dans l'introduction, nous devrons avoir deux attitudes différentes : si l'on ne se privera pas de se servir de toutes les propriétés connues de $\mathbb{N}$, pour celles de ces propriétés qui sont vraies dans tous les autres modèles de $\mathcal{P}$, il nous faudra, du moins en principe, les démontrer, parfois laborieusement, à partir de $\mathcal{P}$.

Il y a dans ce chapitre beaucoup de codages particulièrement indigestes. Le lecteur qui est persuadé que ces codages sont possibles et permettent bien d'obtenir les résultats attendus peut naturellement se dispenser de les lire de façon detaillée.

1. LES AXIOMES DE PEANO

Les axiomes

1.1 Le langage $\mathcal{L}_0$ qui va nous permettre de décrire l'arithmétique est un langage fini comportant quatre symboles :

- un symbole de constante : $\underline{0}$;
- un symbole de fonction unaire : $\underline{S}$;
- deux symboles de fonction binaire : $\underline{+}$ et $\underline{\times}$.

(Attention ! Le symbole $\underline{+}$ est le symbole + qui a été souligné, pour bien le distinguer de l'opération $+$. Il n'a rien à voir avec le signe « plus ou moins ».)

On convient ici d'enfreindre les règles d'écriture des termes du langage $\mathcal{L}_0$, afin de retrouver des notations plus familières ($v_0 \underline{+} v_1$ et $v_0 \underline{\times} v_1$ au lieu, respectivement, de $\underline{+}v_0v_1$ et $\underline{\times}v_0v_1$). Cela exige clairement l'utilisation de parenthèses dans l'écriture des termes (voir nos commentaires au chapitre 3 (2.1)). Pour tout problème de syntaxe relatif aux formules de l'arithmétique, on a toujours la possibilité de revenir à l'écriture officielle qui, seule, fait foi.

Dorénavant, lorsqu'on parlera de $\mathbb{N}$, il s'agira de la $\mathcal{L}_0$-structure dont l'ensemble de base est l'ensemble des entiers naturels et où $\underline{0}$ est interprété par l'entier $\mathbf{0}$, $\underline{S}$ par la fonction successeur $S = \lambda n.n + 1$, $\underline{+}$ par l'addition et $\underline{\times}$ par la multiplication.

Les axiomes de Peano, dont l'ensemble sera noté $\mathcal{P}$, sont les sept axiomes A_1 à A_7 ci-dessous, ainsi qu'une infinité d'axiomes que l'on appellera le **schéma d'induction** et que l'on notera SI.

A_1 : $\forall v_0 \neg \underline{S}v_0 \simeq \underline{0}$

A_2 : $\forall v_0 \exists v_1 (\neg v_0 \simeq \underline{0} \Rightarrow \underline{S} v_1 \simeq v_0)$
A_3 : $\forall v_0 \forall v_1 (\underline{S} v_0 \simeq \underline{S} v_1 \Rightarrow v_0 \simeq v_1)$
A_4 : $\forall v_0\ v_0 \underline{+} \underline{0} \simeq v_0$
A_5 : $\forall v_0 \forall v_1\ v_0 \underline{+} \underline{S} v_1 \simeq \underline{S}(v_0 \underline{+} v_1)$
A_6 : $\forall v_0\ v_0 \underline{\times} \underline{0} \simeq \underline{0}$
A_7 : $\forall v_0 \forall v_1\ v_0 \underline{\times} \underline{S} v_1 \simeq (v_0 \underline{\times} v_1) \underline{+} v_0$.

Enfin, le schéma d'induction est l'ensemble de toutes les formules de $\mathscr{L}_0$ qui sont de la forme :

$$\text{SI}: \quad \forall v_1 \forall v_2 \ldots \forall v_n ((F[\underline{0}, v_1, v_2, \ldots, v_n] \wedge \forall v_0 (F[v_0, v_1, \ldots, v_n] \Rightarrow F[\underline{S} v_0, v_1, \ldots, v_n])) \Rightarrow \forall v_0 F[v_0, v_1, \ldots, v_n])$$

où n est un entier et $F[v_0, v_1, \ldots, v_n]$ est n'importe quelle formule de $\mathscr{L}_0$ ne comportant aucune variable libre autre que $v_0, v_1, \ldots, v_n$.

REMARQUE : Lorsqu'on voudra prouver, en utilisant SI, qu'une formule $F[v_0, v_1, \ldots, v_n]$ est démontrable à partir de $\mathscr{P}$, il suffira d'établir les deux faits suivants :

- $\mathscr{P} \vdash \forall v_1 \forall v_2 \ldots \forall v_n\, F[\underline{0}, v_1, v_2, \ldots, v_n]$;

(ce sera l'**étape initiale** de l'induction, celle qui consiste à « faire $v_0 = \mathbf{0}$ » dans F) ;

- $\mathscr{P} \vdash \forall v_0 \forall v_1 \forall v_2 \ldots \forall v_n\, (F[v_0, v_1, \ldots, v_n] \Rightarrow F[\underline{S} v_0, v_1, \ldots, v_n])$;

(ce sera l'**étape d'induction**).

1.2 Il est visible que $\mathbb{N}$, en tant que $\mathscr{L}_0$-structure, est un modèle de $\mathscr{P}$. C'est ce qu'on appelle habituellement le **modèle standard** de $\mathscr{P}$. On va d'abord montrer que ce n'est pas le seul :

THEOREME : *Il existe des modèles de $\mathscr{P}$ qui ne sont pas isomorphes à $\mathbb{N}$.*

Ꙫ Définissons, pour chaque entier n, le terme $\underline{n} = \underline{S}\,\underline{S} \ldots \underline{S}\,\underline{0}$ composé de n occurrences du symbole $\underline{S}$ suivies du symbole $\underline{0}$. Dans une $\mathscr{L}_0$-structure, on dira qu'un élément est standard si c'est l'interprétation d'un terme de la forme $\underline{n}$ avec $n \in \mathbb{N}$. On voit que, dans le modèle standard (et dans tout modèle qui lui est isomorphe), tout élément est standard. Considérons un nouveau langage $\mathscr{L}$ obtenu en ajoutant à $\mathscr{L}_0$ un nouveau symbole de constante c, et soit T la théorie suivante :

$$T = \{\neg c \simeq \underline{n}\ ;\ n \in \mathbb{N}\} \cup \mathscr{P}.$$

Tout sous-ensemble fini de T admet un modèle ; en effet, soit T_0 un tel sous-ensemble ; il est inclus dans un ensemble de la forme :

$$\{\neg c \simeq \underline{n}\ ;\ n \in I\} \cup \mathscr{P},$$

où I est un sous-ensemble fini de $\mathbb{N}$; on peut faire de $\mathbb{N}$ une $\mathscr{L}$-structure en interprétant

c par n'importe quel entier ; si on prend soin de l'interpréter par un entier n'appartenant pas à I, alors on obtient un modèle de T_0. On peut donc appliquer le théorème de compacité (chapitre 4, 2.7) et en déduire qu'il existe un modèle $\mathfrak{M}$ de T. Ce modèle $\mathfrak{M}$ est aussi évidemment un modèle de $\mathscr{P}$ et il contient un point, à savoir l'interprétation de c, qui n'est pas standard. Le réduit de $\mathfrak{M}$ à $\mathscr{L}_0$ (qui, rappelons-le, est la $\mathscr{L}_0$-structure qui est obtenue naturellement à partir de $\mathfrak{M}$ en oubliant l'interprétation de c) est donc un modèle non standard de $\mathscr{P}$.

☺

1.3 Presque tous les théorèmes d'arithmétique pouvant s'exprimer sous forme d'une formule du premier ordre de $\mathscr{L}_0$ peuvent en fait se démontrer à partir de $\mathscr{P}$ (même si leur démonstration classique utilise des notions n'appartenant pas à l'arithmétique). Pour montrer comment fonctionnent ces axiomes, et en particulier le schéma d'induction, on va voir que, dans les modèles de $\mathscr{P}$, l'addition et la multiplication sont associatives et commutatives, et d'autres propriétés du même genre. On constatera que ces simples faits réclament une preuve assez longue.

THEOREME : *Dans tout modèle $\mathfrak{M}$ de $\mathscr{P}$, l'addition et la multiplication sont associatives et commutatives et la multiplication est distributive par rapport à l'addition ; de plus :*

- *tout élément est régulier pour l'addition :*

$$\mathfrak{M} \models \forall v_0 \forall v_1 \forall v_2((v_0 \underline{+} v_1 \simeq v_0 \underline{+} v_2) \Rightarrow v_1 \simeq v_2) ;$$

- *tout élément non nul est régulier pour la multiplication :*

$$\mathfrak{M} \models \forall v_0 \forall v_1 \forall v_2((\neg v_0 \simeq \underline{0} \land v_0 \underline{\times} v_1 \simeq v_0 \underline{\times} v_2) \Rightarrow v_1 \simeq v_2).$$

- *la formule $\exists v_2(v_2 \underline{+} v_0 \simeq v_1)$ définit un ordre total sur $\mathfrak{M}$, et cet ordre est compatible avec l'addition et la multiplication.*

☺ Ce théorème est conséquence des vingt-quatre (!) faits qui suivent.

(1) $\mathscr{P} \vdash \forall v_0\, \underline{0} \underline{+} v_0 \simeq v_0$.

En utilisant A_4 et A_5 on voit que :

$$\mathscr{P} \vdash \underline{0} \underline{+} \underline{0} \simeq \underline{0} \land \forall v_0(\underline{0} \underline{+} v_0 \simeq v_0 \Rightarrow \underline{0} \underline{+} \underline{S}v_0 \simeq \underline{S}v_0).$$

On utilise alors le schéma SI dans le cas particulier où la formule F est la formule $\underline{0} \underline{+} v_0 \simeq v_0$, et on en déduit :

$$\mathscr{P} \vdash \forall v_0\, \underline{0} \underline{+} v_0 \simeq v_0.$$

(2) $\mathscr{P} \vdash \forall v_0 \forall v_1\, \underline{S}(v_1 \underline{+} v_0) \simeq \underline{S}v_1 \underline{+} v_0$.

Tout d'abord, par A_4 (deux fois) :

$$\mathscr{P} \vdash \underline{S}(v_1 \underline{+} \underline{0}) \simeq \underline{S}v_1 \underline{+} \underline{0}.$$

D'autre part, par A_5 :

$$\mathscr{P} \vdash \underline{S}(v_1 \underline{+} \underline{S}v_0) \simeq \underline{S}\, \underline{S}(v_1 \underline{+} v_0) \wedge \underline{S}v_1 \underline{+} \underline{S}v_0 \simeq \underline{S}(\underline{S}v_1 \underline{+} v_0),$$

et donc $\mathscr{P} \vdash \underline{S}(v_1 \underline{+} v_0) \simeq \underline{S}v_1 \underline{+} v_0 \Longrightarrow \underline{S}(v_1 \underline{+} \underline{S}v_0) \simeq \underline{S}v_1 \underline{+} \underline{S}v_0$,

et on conclut en utilisant SI.

(3) $\mathscr{P} \vdash \forall v_0\ \underline{1} \underline{+} v_0 \simeq \underline{S}v_0$.

(On rappelle que $\underline{1}$ est une notation pour le terme $\underline{S}\ \underline{0}$.)

Il résulte clairement de (2) que :

$$\mathscr{P} \vdash \underline{S}(\underline{0} \underline{+} v_0) \simeq \underline{1} \underline{+} v_0 ;$$

on conclut avec (1).

(4) $\mathscr{P} \vdash \forall v_0 \forall v_1\ v_0 \underline{+} v_1 \simeq v_1 \underline{+} v_0$.

Par A_4 et (1), ceci est vrai lorsque $v_1 = \underline{0}$. D'autre part, par A_5 :

$$\mathscr{P} \vdash v_0 \underline{+} \underline{S}v_1 \simeq \underline{S}(v_0 \underline{+} v_1),$$

et par (2) :

$$\mathscr{P} \vdash \underline{S}v_1 \underline{+} v_0 \simeq \underline{S}(v_1 \underline{+} v_0).$$

Il suffit donc d'appliquer SI.

(5) $\mathscr{P} \vdash \forall v_0 \forall v_1 \forall v_2\ v_0 \underline{+} (v_1 \underline{+} v_2) \simeq (v_0 \underline{+} v_1) \underline{+} v_2$.

C'est encore le schéma d'induction qui va nous donner la démonstration : pour l'étape initiale (« $v_2 = \mathbf{0}$ »), l'égalité se déduit facilement de A_4 ; par A_5, on voit que :

$$\mathscr{P} \vdash v_0 \underline{+} (v_1 \underline{+} \underline{S}v_2) \simeq v_0 \underline{+} \underline{S}(v_1 \underline{+} v_2) \simeq \underline{S}(v_0 \underline{+} (v_1 \underline{+} v_2)),$$

et $\mathscr{P} \vdash (v_0 \underline{+} v_1) \underline{+} \underline{S}v_2 \simeq \underline{S}((v_0 \underline{+} v_1) \underline{+} v_2)$.

Passons maintenant à la multiplication :

(6) $\mathscr{P} \vdash \forall v_0\ \underline{0} \underline{\times} v_0 \simeq \underline{0}$.

En effet, par A_6 :

$$\mathscr{P} \vdash \underline{0} \underline{\times} \underline{0} \simeq \underline{0}$$

et par A_7 :

$$\mathscr{P} \vdash \underline{0} \underline{\times} \underline{S}v_0 \simeq (\underline{0} \underline{\times} v_0) \underline{+} \underline{0},$$

et (6) se déduit encore par SI et A_4.

(7) $\mathscr{P} \vdash \forall v_0\ v_0 \underline{\times} \underline{1} \simeq v_0$.

Par A_7, A_6 et (1).

(8) $\mathscr{P} \vdash \forall v_0 \underline{1} \underline{\times} v_0 \simeq v_0$.

Par SI : le cas « $v_0 = \mathbf{0}$ » relève de A_6 ; puis, A_7, A_5 et A_4 permettent de voir que :

$$\mathscr{P} \vdash \underline{1} \underline{\times} \underline{S}v_0 \simeq \underline{S}(\underline{1} \underline{\times} v_0).$$

(9) $\mathscr{P} \vdash \forall v_0 \forall v_1 \forall v_2\, v_0 \underline{\times} (v_1 \underline{+} v_2) \simeq (v_0 \underline{\times} v_1) \underline{+} (v_0 \underline{\times} v_2)$.

Encore par SI : pour l'étape « $v_2 = 0$ », c'est une conséquence de A_6 et de A_4 ; d'autre part :

$$\mathscr{P} \vdash v_0 \underline{\times} (v_1 \underline{+} \underline{S}v_2) \simeq (v_0 \underline{\times} (v_1 \underline{+} v_2)) \underline{+} v_0 \text{ par } A_5 \text{ et } A_7,$$

et, si $\mathscr{P} \vdash (v_0 \underline{\times} (v_1 \underline{+} v_2)) \underline{+} v_0 \simeq ((v_0 \underline{\times} v_1) \underline{+} (v_0 \underline{\times} v_2)) \underline{+} v_0$ (hypothèse d'induction), alors :

$$\mathscr{P} \vdash ((v_0 \underline{\times} v_1) \underline{+} (v_0 \underline{\times} v_2)) \underline{+} v_0 \simeq (v_0 \underline{\times} v_1) \underline{+} ((v_0 \underline{\times} v_2) \underline{+} v_0) \text{ par (5)},$$

et enfin : $\mathscr{P} \vdash (v_0 \underline{\times} v_1) \underline{+} ((v_0 \underline{\times} v_2) \underline{+} v_0) \simeq (v_0 \underline{\times} v_1) \underline{+} (v_0 \underline{\times} \underline{S}v_2)$ par A_7.

(10) $\mathscr{P} \vdash \forall v_0 \forall v_1 \forall v_2 (v_0 \underline{\times} v_1) \underline{\times} v_2 \simeq v_0 \underline{\times} (v_1 \underline{\times} v_2)$.

SI encore : pour l'étape « $v_2 = 0$ », c'est vrai par A_6 ; puis, par A_7, on a :

$$\mathscr{P} \vdash (v_0 \underline{\times} v_1) \underline{\times} \underline{S}v_2 \simeq ((v_0 \underline{\times} v_1) \underline{\times} v_2) \underline{+} (v_0 \underline{\times} v_1),$$

et par A_7 et (9) :

$$\mathscr{P} \vdash v_0 \underline{\times} (v_1 \underline{\times} \underline{S}v_2) \simeq v_0 \underline{\times} ((v_1 \underline{\times} v_2) \underline{+} v_1) \simeq (v_0 \underline{\times} (v_1 \underline{\times} v_2)) \underline{+} (v_0 \underline{\times} v_1) ;$$

on conclut avec (4).

(11) $\mathscr{P} \vdash \forall v_0 \forall v_1\, v_0 \underline{\times} v_1 \simeq v_1 \underline{\times} v_0$.

On commence à montrer avec le même genre de preuve utilisant SI que :

$$\mathscr{P} \vdash \forall v_0 \forall v_1\, \underline{S}v_0 \underline{\times} v_1 \simeq (v_0 \underline{\times} v_1) \underline{+} v_1 ,$$

puis, on utilise encore SI.

(12) $\mathscr{P} \vdash \forall v_0 \forall v_1 \forall v_2 (v_0 \underline{+} v_2 \simeq v_1 \underline{+} v_2 \Longrightarrow v_0 \simeq v_1)$.

On utilise SI : A_4 pour l'étape « $v_2 = 0$ », puis A_5 et A_3.

(13) $\mathscr{P} \vdash \forall v_0 \forall v_1 (\neg v_1 \simeq \underline{0} \Longrightarrow \neg v_0 \underline{+} v_1 \simeq \underline{0})$.

En effet, par A_2 et A_5 :

$$\mathscr{P} \vdash \neg v_1 \simeq \underline{0} \Longrightarrow \exists v_2 (v_1 \simeq \underline{S}v_2 \wedge v_0 \underline{+} v_1 \simeq \underline{S}(v_0 \underline{+} v_2)),$$

et : $\mathscr{P} \vdash \neg \underline{S}(v_0 \underline{+} v_2) \simeq \underline{0}$ par A_1.

(14) $\mathscr{P} \vdash \forall v_0 \forall v_1 (v_0 \underline{+} v_1 \simeq \underline{0} \Longrightarrow (v_0 \simeq \underline{0} \wedge v_1 \simeq \underline{0}))$.

Par (13) et A_4.

(15) $\mathscr{P} \vdash \forall v_0 \forall v_1 (v_0 \underline{+} v_1 \simeq v_0 \Longrightarrow v_1 \simeq \underline{0})$.

Par (12), A_4 et (4).

La suite au prochain numéro ...

L'ordre sur les entiers

1.4 NOTATION : Dorénavant, $v_0 \leqslant v_1$ sera une abréviation pour la formule $\exists v_2(v_2 \underline{+} v_0 \simeq v_1)$ et $v_0 < v_1$ une abréviation pour $(v_0 \leqslant v_1 \wedge \neg v_0 \simeq v_1)$; les expressions $v_0 \geqslant v_1$ et $v_0 > v_1$ seront respectivement synonymes de $v_1 \leqslant v_0$ et $v_1 < v_0$.

On va montrer que la relation $\leqslant$ est une relation d'ordre total dans tous les modèles de $\mathscr{P}$, et que, de plus, elle est compatible avec l'addition et la multiplication. Evidemment, dans le modèle standard, $\leqslant$ est l'ordre naturel sur les entiers. Notons que nous confondons abusivement ici $\leqslant$, abréviation dans le langage $\mathscr{L}_0$, et la relation binaire que définit, dans un modèle donné, la formule $v_0 \leqslant v_1$, c'est-à-dire l'ensemble des couples d'éléments du modèle qui satisfont cette formule. On utilisera le fait que, grâce à (4), $\mathscr{P}$ démontre la formule $\forall v_0 \forall v_1(v_0 \leqslant v_1 \Longleftrightarrow \exists v_2(v_0 \underline{+} v_2 \simeq v_1))$.

(16) $\mathscr{P} \vdash \forall v_0(v_0 \leqslant v_0)$.
Parce que $\mathscr{P} \vdash \underline{0} \underline{+} v_0 \simeq v_0$.

(17) $\mathscr{P} \vdash \forall v_0 \forall v_1 \forall v_2((v_0 \leqslant v_1 \wedge v_1 \leqslant v_2) \Longrightarrow v_0 \leqslant v_2)$.
Par (5).

(18) $\mathscr{P} \vdash \forall v_0 \forall v_1((v_0 \leqslant v_1 \wedge v_1 \leqslant v_0) \Longrightarrow v_0 \simeq v_1)$.
Se déduit de (5), (15) et (4), et (14).

(19) $\mathscr{P} \vdash \forall v_0 \forall v_1 \forall v_2(v_0 \underline{+} v_2 \leqslant v_1 \underline{+} v_2 \Longleftrightarrow v_0 \leqslant v_1)$.
Par (5) et (12).

(20) $\mathscr{P} \vdash \forall v_0 \forall v_1(v_0 \leqslant v_1 \vee v_1 \leqslant v_0)$.
Ici, il nous faut encore utiliser SI : c'est clair pour « $v_0 = \mathbf{0}$ » (par (1)). D'autre part, on a successivement :

$\mathscr{P} \vdash \forall v_0 v_0 \leqslant \underline{S} v_0$ (par (3) et la définition de $\leqslant$) ;

(•) $\mathscr{P} \vdash \forall v_0 \forall v_1(v_1 \leqslant v_0 \Longrightarrow v_1 \leqslant \underline{S} v_0)$ (par (17)) ;

$\mathscr{P} \vdash \forall v_0 \forall v_1((v_0 \leqslant v_1 \wedge \neg v_1 \simeq v_0) \Longrightarrow \exists v_2(\neg v_2 \simeq \underline{0} \wedge v_1 \simeq v_0 + v_2))$ (A_4) ;

$\mathscr{P} \vdash \forall v_0 \forall v_1((v_0 \leqslant v_1 \wedge \neg v_1 \simeq v_0) \Longrightarrow \exists v_3 v_1 \simeq v_0 + \underline{S} v_3)$ (A_2) ;

$\mathscr{P} \vdash \forall v_0 \forall v_1((v_0 \leqslant v_1 \wedge \neg v_1 \simeq v_0) \Longrightarrow \exists v_3 v_1 \simeq \underline{S} v_0 + v_3)$ (A_5 et (2)) ;

(••) $\mathscr{P} \vdash \forall v_0 \forall v_1((v_0 \leqslant v_1 \wedge \neg v_1 \simeq v_0) \Longrightarrow \underline{S} v_0 \leqslant v_1)$.

On déduit donc, de (•) et (••), que :

$$\mathscr{P} \vdash \forall v_0(\forall v_1(v_0 \leqslant v_1 \vee v_1 \leqslant v_0) \Longrightarrow \forall v_1(\underline{S} v_0 \leqslant v_1 \vee v_1 \leqslant \underline{S} v_0)),$$

ce qui achève l'étape d'induction.

(21) $\mathscr{P} \vdash \forall v_0 \forall v_1 \forall v_2 (v_0 \leqslant v_1 \Longrightarrow v_0 \underline{\times} v_2 \leqslant v_1 \underline{\times} v_2)$.
Par (9) et (11).

(22) $\mathscr{P} \vdash \forall v_0 \forall v_1 (\neg v_1 \simeq \underline{0} \Longrightarrow v_0 \underline{\times} v_1 \geqslant v_0)$.
On applique A_2 et A_7.

(23) $\mathscr{P} \vdash \forall v_0 \forall v_1 ((\neg v_0 \simeq \underline{0} \wedge \neg v_1 \simeq \underline{0}) \Longrightarrow \neg v_0 \underline{\times} v_1 \simeq \underline{0})$.
On remarque que :

$$\mathscr{P} \vdash \forall v_2 \forall v_3 \underline{S} v_2 \underline{\times} \underline{S} v_3 \simeq \underline{S}((\underline{S} v_2 \underline{\times} v_3) \underline{+} v_2) \quad \text{(par } A_7 \text{ et } A_5\text{)},$$

et on applique ensuite A_2 et A_1.

(24) $\mathscr{P} \vdash \forall v_0 \forall v_1 \forall v_2 (v_0 \underline{\times} v_2 \simeq v_1 \underline{\times} v_2 \Longrightarrow (v_0 \simeq v_1 \vee v_2 \simeq \underline{0}))$.
Soient $\mathfrak{M} = \langle M, 0, S, +, \cdot \rangle$ un modèle de $\mathscr{P}$ et a, b et c des éléments de M tels que $a \cdot c = b \cdot c$. D'après (20), on a $a \leqslant b$ ou $b \leqslant a$; dans le premier cas, par exemple, il existe d tel que $d + a = b$, donc ((11) et (9)) : $b \cdot c = (d \cdot c) + (a \cdot c)$. Par (4) et (15), $d \cdot c = 0$, et on conclut en utilisant (23).

Ceci termine la preuve du théorème 1.3.

☺

1.5 NOTATION : On notera $\mathscr{P}_0$ la théorie constituée des axiomes A_1 à A_7. On remarquera que cette théorie est extrêmemement faible. On ne peut même pas démontrer que l'addition est commutative avec ces axiomes (voir l'exercice 1). On va cependant montrer que tout modèle de $\mathscr{P}_0$ (donc aussi tout modèle de $\mathscr{P}$) « commence » par une structure isomorphe à $\mathbb{N}$. On précise d'abord ce que l'on entend par « commence ».

DEFINITION : *Soient $\mathfrak{M}$ et $\mathfrak{N}$ deux modèles de $\mathscr{P}_0$ et on suppose que $\mathfrak{N}$ est une sous-structure de $\mathfrak{M}$. On dit que $\mathfrak{N}$ est un* **segment initial de $\mathfrak{M}$**, *ou d'une façon équivalente que $\mathfrak{M}$ est une* **extension finale de $\mathfrak{N}$** *si, pour tous points* a *appartenant à $\mathfrak{N}$ et* b *appartenant à $\mathfrak{M}$:*

1) si $\mathfrak{M} \models b \leqslant a$, alors b *appartient à $\mathfrak{N}$;*

2) si $b \notin \mathfrak{N}$, alors $\mathfrak{M} \models a \leqslant b$.

1.6 Il faut être vigilant, car $\mathscr{P}_0$ ne démontre pas que la relation $\leqslant$ est une relation d'ordre (exercice 1). Cependant :

THEOREME : *Soit* $\mathfrak{M}$ *un modèle de* $\mathscr{P}_0$ *; alors le sous-ensemble de* $\mathfrak{M}$ *suivant :*

$\{$ a ; *il existe un entier* n *tel que* a *soit l'interprétation de* $\underline{n}$ *dans* $\mathfrak{M}$ $\}$

est une sous-structure de $\mathfrak{M}$ *qui en est un segment initial et qui est isomorphe à* $\mathbb{N}$.

☹ Les faits (25) à (29) qui suivent montrent que l'application φ de $\mathbb{N}$ dans $\mathfrak{M}$ qui à $n \in \mathbb{N}$ fait correspondre l'interprétation de $\underline{n}$ dans $\mathfrak{M}$ est un homomorphisme injectif. Les propriétés (30) et (31) montrent que l'image de cet homomorphisme est un segment initial de $\mathfrak{M}$. Une petite remarque avant de commencer la preuve : ces faits feront intervenir les entiers (les vrais !) et le fait que $\mathscr{P}_0$ ne contienne pas SI ne nous empêchera absolument pas de faire des démonstrations par récurrence sur ces entiers.

(25) *Pour tout entier* n, *on a :*

$\mathscr{P}_0 \vdash \underline{n+1} \simeq \underline{S}\ \underline{n}$.

En fait, il n'y a rien à démontrer : $\underline{n+1}$ et $\underline{S}\ \underline{n}$ représentent le même terme, constitué de $n+1$ occurrences du symbole $\underline{S}$, puis d'une occurrence du symbole $\underline{0}$.

(26) *Pour tous entiers* m *et* n, *on a :*

$\mathscr{P}_0 \vdash \underline{m}\ \underline{+}\ \underline{n} \simeq \underline{m+n}$.

Cela se fait par récurrence sur n : pour $n = 0$, on a bien :

$$\mathscr{P}_0 \vdash \underline{m}\ \underline{+}\ \underline{0} \simeq \underline{m} \text{ (par } A_4\text{).}$$

Pour n+1, en supposant $\mathscr{P}_0 \vdash \underline{m}\ \underline{+}\ \underline{n} \simeq \underline{m+n}$, on a :

$$\mathscr{P}_0 \vdash \underline{n+1} \simeq \underline{S}\ \underline{n} \ \text{ et } \ \mathscr{P}_0 \vdash \underline{m+n+1} \simeq \underline{S}\ \underline{m+n} \quad \text{(par (25))},$$

et : $\mathscr{P}_0 \vdash \underline{m}\ \underline{+}\ \underline{S}\ \underline{n} \simeq \underline{S}(\underline{m}\ \underline{+}\ \underline{n}) \quad \text{(par } A_5\text{)}$,

et tout cela réuni donne :

$$\mathscr{P}_0 \vdash \underline{m}\ \underline{+}\ \underline{n+1} \simeq \underline{m+n+1} \ .$$

(27) *Pour tous entiers* m *et* n, *on a :*

$\mathscr{P}_0 \vdash \underline{m}\ \underline{\times}\ \underline{n} \simeq \underline{m \cdot n}$.

On raisonne encore par récurrence sur n : pour $n = 0$, c'est A_6. D'autre part :

$$\mathscr{P}_0 \vdash \underline{m}\ \underline{\times}\ \underline{n+1} \simeq (\underline{m}\ \underline{\times}\ \underline{n})\ \underline{+}\ \underline{m} \quad \text{(par } A_7 \text{ et (25))} \ ;$$

par hypothèse de récurrence :

$$\mathscr{P}_0 \vdash \underline{m}\ \underline{\times}\ \underline{n} \simeq \underline{m \cdot n},$$

et par (26) :

$$\mathscr{P}_0 \vdash \underline{m \cdot n}\ \underline{+}\ \underline{m} \simeq \underline{m \cdot (n+1)}.$$

(28) *Pour tout entier* n *non nul, on a :*

$\mathscr{P}_0 \vdash \neg \underline{n} \simeq \underline{0}$.

Soit $m = n - 1$; d'après (25) : $\mathscr{P}_0 \vdash \underline{n} \simeq \underline{S}\ \underline{m}$;
on conclut grâce à A_1.

(29) *Pour tous entiers* m *et* n *distincts, on a :*

$\mathscr{P}_0 \vdash \neg \underline{m} \simeq \underline{n}$.

Par récurrence sur $\inf(m,n)$: si l'un des entiers m ou n est nul, c'est le lemme précédent. Sinon, par (25) : $\mathscr{P}_0 \vdash \underline{m} \simeq \underline{n} \Longrightarrow \underline{S}\ \underline{m-1} \simeq \underline{S}\ \underline{n-1}$, et donc, avec A_3 :

$$\mathscr{P}_0 \vdash \underline{m} \simeq \underline{n} \Longrightarrow \underline{m-1} \simeq \underline{n-1} \ ;$$

on conclut grâce à l'hypothèse de récurrence.

(30) *Pour tout entier* n, *on a :*

$\mathscr{P}_0 \vdash \forall v_0(v_0 \leqslant \underline{n} \Longrightarrow (v_0 \simeq \underline{0} \vee v_0 \simeq \underline{1} \vee \ldots \vee v_0 \simeq \underline{n}))$.

Par récurrence sur n : voyons d'abord pour $n = 0$. Il faut montrer que :

$$\mathscr{P}_0 \vdash \forall v_0 \forall v_1(v_1 \,\underline{+}\, v_0 \simeq \underline{0} \Longrightarrow v_0 \simeq \underline{0}).$$

On utilise (14) (dans lequel on remarque que SI n'intervient pas, pas plus que dans (13) : on peut donc y remplacer $\mathscr{P}$ par $\mathscr{P}_0$) ; on a donc :

$$\mathscr{P}_0 \vdash \forall v_0 \forall v_1(v_0 \,\underline{+}\, v_1 \simeq \underline{0} \Longrightarrow (v_0 \simeq \underline{0} \wedge v_1 \simeq \underline{0})).$$

Supposons donc la propriété vraie pour n et montrons-la pour n+1 ; soient donc $\mathfrak{M}$ un modèle de $\mathscr{P}_0$ et a un point de $\mathfrak{M}$, tels que $\mathfrak{M} \models a \leqslant \underline{n+1}$. Il suffit de montrer qu'il existe $p \in \mathbb{N}$ tel que $p \leqslant n+1$ et $\mathfrak{M} \models a \simeq \underline{p}$.

Il existe un point b de $\mathfrak{M}$ tel que $\mathfrak{M} \models b \,\underline{+}\, a \simeq \underline{S}\underline{n}$; si $a = \underline{0}$, c'est fini ; sinon, par A_2, il existe un point c de $\mathfrak{M}$ tel que $\mathfrak{M} \models a \simeq \underline{S}c$; par A_5 et A_3, on voit que $\mathfrak{M} \models b \,\underline{+}\, c \simeq \underline{n}$, donc $\mathfrak{M} \models c \leqslant \underline{n}$, et on peut utiliser l'hypothèse de récurrence : il existe $m \leqslant n$ tel que $\mathfrak{M} \models c = \underline{m}$, d'où $\mathfrak{M} \models \underline{S}c = \underline{S}\underline{m}$, c'est-à-dire $\mathfrak{M} \models a = \underline{m+1}$.

(31) *Pour tout entier* n, *on a :*

$\mathscr{P}_0 \vdash \forall v_0(v_0 \leqslant \underline{n} \vee \underline{n} \leqslant v_0)$.

Par récurrence sur n : pour $n = 0$, c'est immédiat par A_4 et la définition de $\leqslant$. Supposons la propriété vraie pour n. Considérons un modèle $\mathfrak{M}$ de $\mathscr{P}_0$ et un point $a \in \mathfrak{M}$. Il s'agit de montrer que $\mathfrak{M} \models a \leqslant \underline{n+1}$ ou $\mathfrak{M} \models \underline{n+1} \leqslant a$. Si $a = \underline{0}$, c'est clair. Sinon, il existe $b \in \mathfrak{M}$ tel que $\mathfrak{M} \models a = \underline{S}b$; par hypothèse de récurrence, on a alors $\mathfrak{M} \models b \leqslant \underline{n}$ ou $\mathfrak{M} \models \underline{n} \leqslant b$: dans le premier cas, il existe $c \in \mathfrak{M}$ tel que $\mathfrak{M} \models c \,\underline{+}\, b = \underline{n}$, donc, par A_5 et (25), $\mathfrak{M} \models c \,\underline{+}\, a = \underline{n+1}$, d'où $\mathfrak{M} \models a \leqslant \underline{n+1}$; dans le deuxième cas, il existe $d \in \mathfrak{M}$ tel que $\mathfrak{M} \models d \,\underline{+}\, \underline{n} = b$, donc $\mathfrak{M} \models d \,\underline{+}\, \underline{n+1} = a$, d'où $\mathfrak{M} \models \underline{n+1} \leqslant a$.

☺

On trouvera dans l'exercice 2 quelques propriétés supplémentaires des modèles

2. LES FONCTIONS REPRESENTABLES

2.1 Rappelons que $\mathfrak{F}_p$ désigne l'ensemble des fonctions totales de $\mathbb{N}^p$ dans $\mathbb{N}$.

DEFINITION 1 : *Soient* $f \in \mathfrak{F}_p$ *et* $F[v_0,v_1,v_2,\dots,v_p]$ *une formule de* $\mathscr{L}_0$ *qui n'a pas de variables libres en dehors de* $v_0,v_1,v_2,\dots,v_p$. *On dit que* $F[v_0,v_1,v_2,\dots,v_p]$ ***représente*** f *si, pour tout* p-*uple d'entiers* $(n_1,n_2,\dots,n_p)$, *on a :*

$$\mathscr{P}_0 \vdash \forall v_0(F[v_0,\underline{n}_1,\underline{n}_2,\dots,\underline{n}_p] \Longleftrightarrow v_0 \simeq \underline{f(n_1,n_2,\dots,n_p)}).$$

On dit que la fonction f *est* ***représentable*** *s'il existe une formule qui la représente.*

Dire qu'une formule F représente f, c'est donc dire que, pour tout modèle $\mathfrak{M}$ de $\mathscr{P}_0$ et toute suite d'entiers $(n_1,n_2,\dots,n_p)$, il existe un et un seul élément x de $\mathfrak{M}$ satisfaisant $F[x,\underline{n}_1,\underline{n}_2,\dots,\underline{n}_p]$ et que cet élément, c'est l'élément (standard) qui interprète le terme $\underline{f(n_1,n_2,\dots,n_p)}$ qui, rappelons-le, est constitué du symbole $\underline{S}$ répété $f(n_1,n_2,\dots,n_p)$ fois suivi de $\underline{0}$. On peut adapter cette définition aux sous-ensembles :

DEFINITION 2 : *Soient* $A \subseteq \mathbb{N}^p$ *et* $F[v_1,v_2,\dots,v_p]$ *une formule qui n'a pas de variables libres en dehors de* $v_1,v_2,\dots,v_p$. *On dit que* F ***représente*** A *si, pour tout* p-*uple d'entiers* $(n_1,n_2,\dots,n_p)$, *on a :*

- *si* $(n_1,n_2,\dots,n_p) \in A$ *alors* $\mathscr{P}_0 \vdash F[\underline{n}_1,\underline{n}_2,\dots,\underline{n}_p]$;
- *si* $(n_1,n_2,\dots,n_p) \notin A$ *alors* $\mathscr{P}_0 \vdash \neg F[\underline{n}_1,\underline{n}_2,\dots,\underline{n}_p]$.

On dit que l'ensemble A *est* ***représentable*** *s'il existe une formule qui le représente.*

REMARQUE : Un ensemble $A \subseteq \mathbb{N}^p$ est représentable si et seulement si sa fonction caractéristique l'est : on vérifiera que, si F représente A, la formule

$$(F[v_1,v_2,\dots,v_p] \wedge v_0 \simeq \underline{1}) \vee (\neg F[v_1,v_2,\dots,v_p] \wedge v_0 \simeq \underline{0})$$

représente la fonction caractéristique de A ; réciproquement, si $G[v_0,v_1,v_2,\dots,v_p]$ représente la fonction caractéristique de A, alors $G[\underline{1},v_1,v_2,\dots,v_p]$ représente A.

Donnons quelques exemples de fonctions représentables avec les formules correspondantes :

• La fonction successeur est représentée par la formule $v_0 \simeq \underline{S}v_1$ (1.4, (25)).

• L'addition $\lambda xy . x + y$ est représentée par la formule $v_0 \simeq v_1 \underline{+} v_2$ (1.4, (26)).

• La multiplication $\lambda xy . x \cdot y$ est représentée par la formule $v_0 \simeq v_1 \underline{\times} v_2$ (1.4, (27)).

• Les fonctions projection sont aussi représentables : la fonction P_p^i est représentée par la formule $v_0 \simeq v_i$.

• La fonction constante égale à n est représentée par la formule $v_0 \simeq \underline{n}$.

2.2 En fait, toutes les fonctions récursives sont représentables :

THEOREME DE REPRESENTATION : *Toute fonction récursive (totale) est représentable.*

☹ Avec ce que l'on a déjà vu, il suffit de montrer que l'ensemble des fonctions représentables est clos par composition, par le schéma μ total et par récurrence (voir la dernière remarque de 3.14 au chapitre 5). C'est l'objet des lemmes qui suivent.

LEMME 1 : *L'ensemble des fonctions représentables est clos par composition.*

☹ Soient $f_1,f_2,\dots,f_n \in \mathfrak{F}_p$ et $g \in \mathfrak{F}_n$ et supposons que, pour chaque i compris entre 1 et n, f_i soit représentée par $F_i[v_0,v_1,v_2,\dots,v_p]$ et que g soit représentée par $G[v_0,v_1,v_2,\dots,v_n]$. Une vérification immédiate montre que $g(f_1,f_2,\dots,f_n)$ est représentée par :

$$\exists w_1 \exists w_2 \dots \exists w_n (G[v_0,w_1,w_2,\dots,w_n] \wedge \bigwedge_{1 \leqslant i \leqslant n} F_i[w_i,v_1,v_2,\dots,v_p]).$$

☺

LEMME 2 : *Soit* $A \subseteq \mathbb{N}^{p+1}$ *un ensemble représentable tel que la fonction* $f(x_1,x_2,\dots,x_p) = \mu y\ ((y,x_1,x_2,\dots,x_p) \in A)$ *soit totale ; alors* f *est représentable.*

☹ Soit $F[v_0,v_1,\dots,v_p]$ une formule représentant A ; on va voir que la formule :

$$G = F[v_0,v_1,v_2,\dots,v_p] \wedge \forall w < v_0\ \neg F[w,v_1,v_2,\dots,v_p]$$

représente f. En effet, soit $\mathfrak{M}$ un modèle de $\mathscr{P}_0$ et $n_1,n_2,\dots,n_p$ des entiers. Il s'agit de montrer que b, interprétation de $\underline{f(n_1,n_2,\dots,n_p)}$ dans $\mathfrak{M}$, est le seul élément de $\mathfrak{M}$ qui satisfait la formule $G[v_0,\underline{n}_1,\underline{n}_2,\dots,\underline{n}_p]$. Premièrement, puisque F représente A, on a :

$$\mathscr{P}_0 \vdash F[b,\underline{n}_1,\underline{n}_2,\ldots,\underline{n}_p],$$

et, puisque $\mathfrak{M}$ est un modèle de $\mathscr{P}_0$, b satisfait $F[v_0,\underline{n}_1,\underline{n}_2,\ldots,\underline{n}_p]$ dans $\mathfrak{M}$. De plus, si c est un élément de $\mathfrak{M}$ qui est inférieur à b, alors, d'après le théorème 1.6, c est un élément standard et, par définition de f, il ne satisfait pas $F[v_0,\underline{n}_1,\underline{n}_2,\ldots,\underline{n}_p]$, donc b satisfait $G[v_0,\underline{n}_1,\underline{n}_2,\ldots,\underline{n}_p]$. Par ailleurs, soit d un élément de $\mathfrak{M}$ qui satisfait $G[v_0,\underline{n}_1,\underline{n}_2,\ldots,\underline{n}_p]$: on ne peut alors avoir, dans $\mathfrak{M}$, ni $d < b$ ni $b < d$; mais comme b est standard, on doit avoir, en vertu du théorème 1.6, $d \leqslant b$ ou $b \leqslant d$, d'où finalement $b = d$.

☺

2.3 On en vient maintenant au point le plus délicat qui est la définition par récurrence. On doit introduire pour cela une fonction astucieuse, connue sous le nom de **fonction β de Gödel**, dont le rôle est de coder les suites finies d'entiers :

LEMME 3 : *Il existe une fonction β à trois variables, qui est récursive primitive et représentable, telle que, pour tout $p \in \mathbb{N}$ et toute suite $(n_1,n_2,\ldots,n_p) \in \mathbb{N}^p$, il existe des entiers a et b tels que, pour tout i compris entre 1 et p, on ait $\beta(i,a,b) = n_i$.*

Avant de démontrer ce lemme, terminons la démonstration du théorème de représentation à l'aide du lemme 3 ; il nous reste à montrer :

LEMME 4 : *Soient $g \in \mathfrak{F}_p$ et $h \in \mathfrak{F}_{p+2}$ deux fonctions représentables ; alors la fonction f définie par récurrence à partir de g et h par :*

- $f(x_1,x_2,\ldots,x_p,0) = g(x_1,x_2,\ldots,x_p)$
- $f(x_1,x_2,\ldots,x_p,x_{p+1}+1) = h(x_1,x_2,\ldots,x_p,x_{p+1},f(x_1,x_2,\ldots,x_p,x_{p+1}))$

est aussi représentable.

☺ Pour écrire que $y = f(x_1,x_2,\ldots,x_p,x_{p+1})$, on va écrire qu'il existe une suite d'entiers $(z(0),z(1),\ldots,z(x_{p+1}))$ telle que :

$$z(0) = g(x_1,x_2,\ldots,x_p)\ ,\ \ z(x_{p+1}) = y,$$

et, pour tout i compris entre 0 et $x_{p+1} - 1$,

$$z(i+1) = h(x_1,x_2,\ldots,x_p,i,z(i))\ .$$

Evidemment, pour dire « il existe une suite... », on dira qu'il existe deux entiers codant cette suite au moyen de la fonction β.

Soient $G[v_0,v_1,\ldots,v_p]$ et $H[v_0,v_1,\ldots,v_{p+2}]$ des formules représentant respectivement les fonctions g et h. Pour la fonction β, il faut être un peu plus précautionneux ; soit

$B[v_0,v_1,v_2,v_3]$ une formule représentant β. Cette fonction est aussi représentée par la formule B' suivante :

$$B'[v_0,v_1,v_2,v_3] = B[v_0,v_1,v_2,v_3] \wedge \forall v_4 < v_0 \neg B[v_4,v_1,v_2,v_3].$$

L'avantage de B' par rapport à B, c'est que, si $\mathfrak{M}$ est un modèle quelconque de $\mathscr{P}_0$, si x est un élément standard de $\mathfrak{M}$ (interprétation de $\underline{n}$ pour un certain entier intuitif n), et si a,b et c sont trois points de $\mathfrak{M}$ tels que :

$$\mathfrak{M} \models B'[x,a,b,c],$$

alors il n'y a dans $\mathfrak{M}$ aucun autre point, standard ou pas, satisfaisant $B'[v_0,a,b,c]$. On va vérifier que la formule $F[v_0,v_1,v_2,\ldots,v_p,v_{p+1}]$ qui suit représente la fonction f :

$$\exists w_1 \exists w_2(\exists w_0(B'[w_0,\underline{1},w_1,w_2] \wedge G[w_0,v_1,v_2,\ldots,v_p]) \wedge B'[v_0,v_{p+1}\underline{+}\underline{1},w_1,w_2] \wedge$$
$$\forall w_3 < v_{p+1} \exists w_4 \exists w_5(B'[w_4,\underline{S}w_3,w_1,w_2] \wedge B'[w_5,\underline{S}\,\underline{S}w_3,w_1,w_2] \wedge H[w_5,v_1,v_2,\ldots,v_p,w_3,w_4])).$$

(Quelques explications pour aider à la lecture de cette formule : les variables w_1 et w_2 représentent des entiers a et b tels que, pour tout i compris entre 0 et x_{p+1}, $f(x_1,x_2,\ldots,x_p,i)$ est égal à $\beta(i+1,a,b)$, w_0 doit prendre la valeur $g(x_1,x_2,\ldots,x_p)$, et si, $0 \leqslant w_3 < n_{p+1}$, alors w_4 doit être égal à $f(x_1,x_2,\ldots,x_p,w_3)$ et w_5 à $f(x_1,x_2,\ldots,x_p,w_3+1)$.)

Soient donc $n_1,n_2,\ldots,n_{p+1}$ des entiers, $\mathfrak{M}$ un modèle de $\mathscr{P}_0$, et c un point de $\mathfrak{M}$. On voit d'abord clair que, si :

$$\mathfrak{M} \models c \simeq \underline{f(n_1,n_2,\ldots,n_p,n_{p+1})},$$

alors $\quad \mathfrak{M} \models F[c,\underline{n}_1,\underline{n}_2,\ldots,\underline{n}_{p+1}]$.

Les valeurs qu'il faut donner aux variables w_1 et w_2 pour témoigner que cette formule est vérifiée, ce sont précisément les interprétations de $\underline{a}$ et $\underline{b}$, où a et b sont des entiers codant la suite :

$$(f(n_1,n_2,\ldots,n_p,0),f(n_1,n_2,\ldots,n_p,1),\ldots,f(n_1,n_2,\ldots,n_p,n_{p+1})),$$

au moyen de la fonction β, et dont l'existence est assurée par le lemme 3.

Réciproquement, supposons que :

$$\mathfrak{M} \models F[c,\underline{n}_1,\underline{n}_2,\ldots,\underline{n}_{p+1}] ;$$

il s'agit de montrer que c est l'élément standard qui interprète $\underline{f(n_1,n_2,\ldots,n_{p+1})}$.

Parce que $F[c,\underline{n}_1,\underline{n}_2,\ldots,\underline{n}_{p+1}]$ est vraie dans $\mathfrak{M}$, on sait qu'il existe des éléments a, b et d dans $\mathfrak{M}$ tels que

$$\mathfrak{M} \models B'[d,\underline{1},a,b] \wedge G[d,\underline{n}_1,\underline{n}_2,\ldots,\underline{n}_p] \wedge B'[c,\underline{n}_{p+1}\underline{+}\underline{1},a,b]$$

et pour tout entier i tel que $0 \leqslant i < n_{p+1}$, il y a des éléments r_i et s_i dans $\mathfrak{M}$ tels que

$$\mathfrak{M} \models B'[r_i,\underline{S}\underline{i},a,b] \wedge B'[s_i,\underline{S}\,\underline{S}\underline{i},a,b] \wedge H[s_i,\underline{n}_1,\underline{n}_2,\ldots,\underline{n}_p,\underline{i},r_i]).$$

Parce que G représente g, $\mathfrak{M} \models d \simeq \underline{g(n_1,n_2,\ldots,n_p)}$. Puisque la formule B' a été choisie de sorte que pour tous x, y, z dans $\mathfrak{M}$, il y ait au plus un point satisfaisant $B'[v_0,x,y,z]$, on voit que $d = r_0$, que $c = s_{n_{p+1}-1}$ et que, pour tout entier i tel que $0 \leqslant i < n_{p+1}$, $r_{i+1} = s_i$. En utilisant la définition de H, on voit ensuite, par récurrence sur $i < n_{p+1}$ que :

$$\mathfrak{M} \models r_i \simeq \underline{f(n_1,n_2,\ldots,n_p,i)},$$

et donc que $\mathfrak{M} \models c \simeq \underline{f(n_1,n_2,\ldots,n_{p+1})}$.

☺

Remarquons que, dans le lemme 3, c'est le fait que β soit représentable qui est difficile à assurer : sinon la fonction δ introduite au chapitre 5, 1.12 conviendrait parfaitement. Cette fonction δ est récursive primitive, et on pourra conclure à la fin qu'elle est représentable, mais pour l'instant, on ne peut l'affirmer.

2.4 ☹ Revenons à la démonstration du lemme 3 : pour définir cette fonction β, on doit utiliser quelques faits élémentaires d'arithmétique et en particulier le résultat classique suivant connu sous le nom de **théorème chinois** :

THEOREME : *Soient* $(b_0,b_1,\ldots,b_n)$ *une suite d'éléments de* $\mathbb{N}$ *premiers entre eux deux à deux et* $(\alpha_0,\alpha_1,\ldots,\alpha_n)$ *une suite de même longueur d'éléments de* $\mathbb{N}$. *Alors il existe* $a \in \mathbb{N}$ *tel que pour, tout* i *compris entre* 0 *et* n, *on ait :*

$$a \textit{ congru à } \alpha_i \textit{ modulo } b_i.$$

(La preuve de ce théorème est donnée dans l'exercice 3.)

Par définition, $\beta(i,a,b)$ est le reste de la division euclidienne de b par $a(i+1)+1$. On voit d'abord sans peine que β est représentée par la formule :

$$B[v_0,v_1,v_2,v_3] = \exists v_4 v_3 \simeq (v_4 \,\underline{\times}\, \underline{S}(v_2 \,\underline{\times}\, \underline{S}v_1)) \,\underline{+}\, v_0 \land v_0 < \underline{S}(v_2 \,\underline{\times}\, \underline{S}v_1).$$

Elle posssède d'autre part la propriété voulue : soit $(\alpha_0,\alpha_1,\ldots,\alpha_n)$ une suite d'entiers. On choisit un entier m supérieur à $n+1$ et tel que, si on pose $a = m!$, a soit au moins égal à tous les α_i. On voit que les entiers $a(i+1)+1$ pour i compris entre 0 et n sont premiers entre eux deux à deux : supposons $0 \leqslant i < j \leqslant n$, et soit c un diviseur premier commun à $a(i+1)+1$ et $a(j+1)+1$; c doit diviser la différence $a(i-j) = m!(i-j)$ et doit donc être inférieur ou égal à m, ce qui est impossible puisqu'il doit aussi diviser $m!(i+1)+1$.

Le théorème chinois nous dit alors qu'il existe un entier b tel que, pour tout i compris entre 0 et n, on ait :

$$b \text{ congru à } \alpha_i \text{ modulo } a(i+1)+1,$$

et, puisque $\alpha_i \leqslant a < a(i+1)+1$, on a bien $\beta(i,a,b) = \alpha_i$.

☺

Ceci termine la démonstration du théorème de représentation.

☺

On en déduit de façon évidente que tout ensemble récursif est représentable. D'autre part, soit $\mathscr{P}'$ une théorie quelconque contenant $\mathscr{P}_0$ (par exemple $\mathscr{P}$). Il est bien clair que, si $f \in \mathfrak{F}_p$ est représentée par la formule F, et si $(n_1,n_2,\ldots,n_p)$ est une suite d'entiers, alors $\mathscr{P}' \vdash \forall v_0(F[v_0,\underline{n}_1,\underline{n}_2,\ldots,\underline{n}_p] \Longleftrightarrow v_0 \simeq \underline{f(n_1,n_2,\ldots,n_p)})$.

3. ARITHMETISATION DE LA SYNTAXE

Codage des formules

3.1 Dans cette section, on va coder les termes et les formules d'un langage fini par des entiers. On pourrait faire ce travail pour n'importe quel langage fini, et même certains langages infinis, mais pour éviter des notations trop compliquées, on se contentera du langage $\mathscr{L}_0$. Notre but est surtout de montrer que l'ensemble des formules universellement valides est récursivement énumérable. Le codage va utiliser les fonctions α_i et β_i^i introduites au chapitre 5, en 1.11. On a aussi besoin du petit lemme suivant :

LEMME : *Soient* p *et* n *des entiers,* $k_1,k_2,\dots,k_n \in \mathfrak{F}_1$, $g \in \mathfrak{F}_p$, $h \in \mathfrak{F}_{n+p+1}$ *des fonctions récursives primitives, et on suppose que, pour tous* $y > 0$ *et* i *compris entre* 1 *et* n, $k_i(y) < y$. *Alors l'unique fonction déterminée par les conditions suivantes :*

- $f(0,x_1,x_2,\dots,x_p) = g(x_1,x_2,\dots,x_p)$;
- $f(y,x_1,x_2,\dots,x_p) = h(y,f(k_1(y),x_1,x_2,\dots,x_p),f(k_2(y),x_1,x_2,\dots,x_p),\dots,$ $f(k_n(y),x_1,x_2,\dots,x_p),x_1,x_2,\dots,x_p))$ *si* $y > 0$;

est récursive primitive.

☹ Il s'agit d'une définition par récurrence qui n'entre pas tout à fait dans le cadre de la définition de 1.2 du chapitre 5. Pour la normaliser, on va utiliser : la fonction Ω définie au chapitre 5, en 1.12 (elle servira à coder la suite des valeurs de $f(i,x_1,x_2,\dots,x_p)$ pour i variant de 0 à y), la fonction π ($\pi(n)$ est le $(n+1)$-ème nombre premier), et la fonction δ (qui permet de décoder Ω). Définissons la fonction φ par :

$$\varphi(y,x_1,x_2,\dots,x_p) = \Omega(f(0,x_1,x_2,\dots,x_p),f(1,x_1,x_2,\dots,x_p),\dots,f(y,x_1,x_2,\dots,x_p)).$$

On voit que φ peut être directement définie par :

- $\varphi(0,x_1,x_2,\dots,x_p) = 2^{g(x_1,x_2,\dots,x_p)}$;
- $\varphi(y+1,x_1,x_2,\dots,x_p) = \varphi(y,x_1,x_2,\dots,x_p).\pi(y+1)^{\gamma}$,

où $\gamma = h(y+1,\delta(k_1(y+1),\varphi(y,x_1,x_2,\dots,x_p)),\delta(k_2(y+1),\varphi(y,x_1,x_2,\dots,x_p)),\dots,$ $\delta(k_n(y+1),\varphi(y,x_1,x_2,\dots,x_p)),x_1,x_2,\dots,x_p)$.

La fonction φ est donc récursive primitive, de même que f puisque :

$$f(y,x_1,x_2,\dots,x_p) = \delta(y,\varphi(y,x_1,x_2,\dots,x_p)).$$

☺

3.2 On peut maintenant passer au codage des termes. L'idée est de coder un terme t par un triplet d'entiers (a,b,c) où la dernière composante c permettra de distinguer si t est un terme élémentaire, ou s'il est de la forme $\underline{S}t_1$, ou s'il est de la forme $t_1 \underline{+} t_2$, ou s'il est de la forme $t_1 \underline{\times} t_2$; les composantes a et b coderont, suivant le cas, le terme élémentaire auquel t est égal ou les termes t_1 et t_2 à partir desquels t est construit. Evidemment, le triplet (a,b,c) sera réduit à un seul entier à l'aide de la fonction α_3.

On définit par induction sur le terme t un entier qu'on notera #t et qu'on appellera le **numéro de Gödel de** t, par les conditions suivantes :

- si $t = \underline{0}$, alors $\#t = \alpha_3(0,0,0)$;
- si $t = v_n$, alors $\#t = \alpha_3(n + 1,0,0)$;
- si $t = \underline{S}t_1$, alors $\#t = \alpha_3(\#t_1,0,1)$;
- si $t = t_1 \underline{+} t_2$, alors $\#t = \alpha_3(\#t_1,\#t_2,2)$;
- si $t = t_1 \underline{\times} t_2$, alors $\#t = \alpha_3(\#t_1,\#t_2,3)$.

LEMME : *L'ensemble* Term $= \{\#t$; t *est un terme de* $\mathscr{L}_0\}$ *est récursif primitif.*

☺ En effet, g, la fonction caractéristique de Term, peut être définie de la façon suivante :

- $g(0) = 1$; $g(1) = 1$;

et, si $x > 1$:

- si $\beta_3^3(x) = 0$ et $\beta_3^2(x) = 0$, alors $g(x) = 1$;
- si $\beta_3^3(x) = 0$ et $\beta_3^2(x) \neq 0$, alors $g(x) = 0$;
- si $\beta_3^3(x) = 1$ et $\beta_3^2(x) \neq 0$, alors $g(x) = 0$;
- si $\beta_3^3(x) = 1$ et $\beta_3^2(x) = 0$, alors $g(x) = g(\beta_3^1(x))$;
- si $\beta_3^3(x) = 2$, alors $g(x) = g(\beta_3^1(x)).g(\beta_3^2(x))$
- si $\beta_3^3(x) = 3$, alors $g(x) = g(\beta_3^1(x)).g(\beta_3^2(x))$
- si $\beta_3^3(x) > 3$, alors $g(x) = 0$.

Or, en se reportant au chapitre 5 (1.11), on voit que, si $x > 1$, $\beta_3^1(x)$, $\beta_3^2(x)$ et $\beta_3^3(x)$ sont strictement inférieurs à x, et on peut donc appliquer le lemme 3.1.

☺

Ce codage est injectif : si $\#t = \#t'$, alors $t = t'$. Le lecteur qui n'en est pas convaincu peut vérifier cela par induction sur t.

3.3 On peut maintenant passer au codage des formules. On utilise le même principe. Les formules atomiques seront repérées par une troisième composante égale à **0** ; la

troisième composante des négations sera égale à 1, celle des conjonctions à 2, etc. Le code d'une formule F sera encore noté # F et appelé **numéro de Gödel de F**. Voici donc la définition par induction de # F :

- si $F = t_1 \simeq t_2$, alors $\# F = \alpha_3(\# t_1, \# t_2, 0)$;
- si $F = \neg F_1$, alors $\# F = \alpha_3(\# F_1, 0, 1)$;
- si $F = (F_1 \wedge F_2)$, alors $\# F = \alpha_3(\# F_1, \# F_2, 2)$;
- si $F = (F_1 \vee F_2)$, alors $\# F = \alpha_3(\# F_1, \# F_2, 3)$;
- si $F = (F_1 \Rightarrow F_2)$, alors $\# F = \alpha_3(\# F_1, \# F_2, 4)$;
- si $F = (F_1 \Longleftrightarrow F_2)$, alors $\# F = \alpha_3(\# F_1, \# F_2, 5)$;
- si $F = \forall v_n F_1$, alors $\# F = \alpha_3(\# F_1, n, 6)$;
- si $F = \exists v_n F_1$, alors $\# F = \alpha_3(\# F_1, n, 7)$.

On a encore :

LEMME : *L'ensemble* Form = { # F ; F *est une formule de* $\mathscr{L}_0$ } *est récursif primitif.*

☹ C'est toujours le même type de preuve. La fonction caractéristique de Term étant g, celle de Form, h, peut être définie par :

- si $\beta_3^3(x) = 0$, alors $h(x) = g(\beta_3^1(x)).g(\beta_3^2(x))$;
- si $\beta_3^3(x) = 1$ et $\beta_3^2(x) \neq 0$, alors $h(x) = 0$.
- si $\beta_3^3(x) = 1$ et $\beta_3^2(x) = 0$, alors $h(x) = h(\beta_3^1(x))$;
- si $\beta_3^3(x) = 2,3,4$ ou 5, alors $h(x) = h(\beta_3^1(x)).h(\beta_3^2(x))$;
- si $\beta_3^3(x) = 6$ ou 7, alors $h(x) = h(\beta_3^1(x))$;
- si $\beta_3^3(x) > 7$, alors $h(x) = 0$.

☺

On remarque que, comme pour les termes, on a un codage injectif.

3.4 Il faut aussi montrer que les opérations que l'on sait effectuer sur les formules, comme les substitutions ou la reconnaissance des variables libres ou liées, correspondent à des fonctions récursives primitives sur les numéros de Gödel.

LEMME 1 : *Les ensembles suivants :*

- Θ_0 = { (# t,n) ; t *est un terme et* v_n *n'a pas d'occurrence dans* t },
- Θ_1 = { (# t,n) ; t *est un terme et* v_n *a au moins une occurrence dans* t },
- Φ_0 = { (# F,n) ; F *est une formule et* v_n *n'a pas d'occurrence dans* F },

• $\Phi_1 = \{(\#F,n)$; F *est une formule et* v_n *n'a pas d'occurrence libre dans* F $\}$,
• $\Phi_2 = \{(\#F,n)$; F *est une formule et* v_n *n'a pas d'occurrence liée dans* F $\}$,
• $\Phi_3 = \{\#F$; F *est une formule close* $\}$,
• $\Phi_4 = \{(\#F,n)$; F *est une formule et* v_n *a au moins une occurrence libre dans* F $\}$,
• $\Phi_5 = \{(\#F,n)$; F *est une formule et* v_n *a au moins une occurrence liée dans* F $\}$,
sont récursifs primitifs.

☹ On se contentera de traiter le cas de Θ_0 et de Φ_1. Les fonctions caractéristiques de Term et de Form seront encore appelées g et h respectivement. La fonction caractéristique de Θ_0, qu'on notera g_0, peut être définie par les conditions suivantes :
• si $\beta_3^3(x) = 0$, alors $g_0(x,y) = 1$ si et seulement si $\beta_3^2(x) = 0$ et $\beta_3^1(x) \neq y + 1$;
• si $\beta_3^3(x) = 1$ et $\beta_3^2(x) \neq 0$, alors $g_0(x,y) = 0$;
• si $\beta_3^3(x) = 1$ et $\beta_3^2(x) = 0$, alors $g_0(x,y) = g_0(\beta_3^1(x),y)$;
• si $\beta_3^3(x) = 2$ ou 3, alors $g_0(x,y) = g_0(\beta_3^1(x),y).g_0(\beta_3^2(x),y)$;
• si $\beta_3^3(x) > 3$, alors $g_0(x,y) = 0$.

Soit maintenant h_1 la fonction caractéristique de Φ_1. Alors :
• si $\beta_3^3(x) = 0$, alors $h_1(x,y) = g_0(\beta_3^1(x),y).g_0(\beta_3^2(x),y)$;
• si $\beta_3^3(x) = 1$ et $\beta_3^2(x) \neq 0$, alors $h_1(x,y) = 0$;
• si $\beta_3^3(x) = 1$ et $\beta_3^2(x) = 0$, alors $h_1(x,y) = h_1(\beta_3^1(x),y)$;
• si $\beta_3^3(x) = 2$, 3, 4 ou 5, alors $h_1(x,y) = h_1(\beta_3^1(x),y).h_1(\beta_3^2(x),y)$;
• si $\beta_3^3(x) = 6$ ou 7 et $\beta_3^2(x) \neq y$, alors $h_1(x,y) = h_1(\beta_3^1(x),y)$;
• si $\beta_3^3(x) = 6$ ou 7 et $\beta_3^2(x) = y$, alors $h_1(x,y) = h(\beta_3^1(x))$;
• si $\beta_3^3(x) > 7$, alors $h_1(x,y) = 0$.

C'est évidemment le lemme 3.1 qui permet de conclure que les ensembles considérés sont récursifs primitifs.
☺

Passons aux substitutions. On obtient sans surprise :

LEMME 2 : *Il existe deux fonctions récursives primitives* $Subs_t$ et $Subs_f$ *à trois variables telles que, si* t *et* u *sont des termes et si* F *est une formule, alors, pour tout entier* n :

$$Subs_t(n,\#t,\#u) = \#u_{t/v_n} ;$$

$$Subs_f(n,\#t,\#F) = \#F_{t/v_n}.$$

(Pour la définition de u_{t/v_n} et F_{t/v_n}, voir chapitre 3, 1.8.)

☹ On utilise encore le lemme 3.1. On définit d'abord la fonction $\mathrm{Subs_t}$ par les conditions suivantes :

- Si $\beta_3^3(x) = 0$, alors :

  $\mathrm{Subs_t}(n,y,x) = x$ si $x \neq \alpha_3(n+1,0,0)$,

  et $\mathrm{Subs_t}(n,y,x) = y$ sinon ;
- si $\beta_3^3(x) = 1$ et $\beta_3^2(x) = 0$, alors $\mathrm{Subs_t}(n,y,x) = \alpha_3(\mathrm{Subs_t}(n,y,\beta_3^1(x)),0,1)$;
- si $\beta_3^3(x) = 2$ ou 3, alors

  $\mathrm{Subs_t}(n,y,x) = \alpha_3(\mathrm{Subs_t}(n,y,\beta_3^1(x)),\mathrm{Subs_t}(n,y,\beta_3^2(x)),\beta_3^3(x))$;
- dans les autres cas, on pose arbitrairement : $\mathrm{Subs_t}(n,y,x) = x$.

Pour la fonction $\mathrm{Subs_f}$, c'est un peu plus compliqué, car la substitution ne doit se faire que pour les occurrences libres de la variable :

- si $\beta_3^3(x) = 0$, alors $\mathrm{Subs_f}(n,y,x) = \alpha_3(\mathrm{Subs_t}(n,y,\beta_3^1(x)),\mathrm{Subs_t}(n,y,\beta_3^2(x)),0)$;
- si $\beta_3^3(x) = 1$ et $\beta_3^2(x) = 0$, alors $\mathrm{Subs_f}(n,y,x) = \alpha_3(\mathrm{Subs_f}(n,y,\beta_3^1(x)),0,1)$;
- si $\beta_3^3(x) = 2$, 3, 4 ou 5, alors $\mathrm{Subs_f}(n,y,x) =$

  $\alpha_3(\mathrm{Subs_f}(n,y,\beta_3^1(x)),\mathrm{Subs_f}(n,y,\beta_3^2(x)),\beta_3^3(x))$;
- si $\beta_3^3(x) = 6$ ou 7, alors :

  $\mathrm{Subs_f}(n,y,x) = x$ si $\beta_3^2(x) = n$,

  et $\mathrm{Subs_f}(n,y,x) = \alpha_3(\mathrm{Subs_f}(n,y,\beta_3^1(x)),\beta_3^2(x),\beta_3^3(x))$ sinon ;
- dans les autres cas, on pose arbitrairement : $\mathrm{Subs_f}(n,y,x) = x$.

☺

Codage des démonstrations

3.5 On en arrive à un point légèrement plus difficile qui est la décidabilité du calcul des propositions. On va revenir à ce calcul momentanément. On a donc, en plus des connecteurs propositionnels, une infinité de variables propositionnelles A_1, A_2, ... On commence par établir un codage des formules propositionnelles analogue à ceux qui précèdent. A une proposition P, on fait correspondre son **numéro de Gödel**, noté $\# P$ et défini comme suit :

- si $P = A_n$, alors $\# P = \alpha_3(n,0,0)$;
- si $P = \neg P_1$, alors $\# P = \alpha_3(\# P_1,0,1)$;
- si $P = (P_1 \wedge P_2)$, alors $\# P = \alpha_3(\# P_1,\# P_2,2)$;
- si $P = (P_1 \vee P_2)$, alors $\# P = \alpha_3(\# P_1,\# P_2,3)$;
- si $P = (P_1 \Longrightarrow P_2)$, alors $\# P = \alpha_3(\# P_1,\# P_2,4)$;
- si $P = (P_1 \Longleftrightarrow P_2)$, alors $\# P = \alpha_3(\# P_1,\# P_2,5)$.

Comme c'est maintenant une habitude, on voit que l'ensemble :

$$\text{Prop} = \{ \# P \ ; \ P \text{ est une proposition} \}$$

est récursif primitif.

THEOREME *(Décidabilité du calcul propositionnel)* : *L'ensemble :*

$$\mathcal{T} = \{ \# P \ ; \ P \textit{ est une tautologie} \}$$

est récursif primitif.

⊖ A chaque entier k, on fait correspondre la distribution de valeurs de vérité λ_k définie de la façon suivante :

$\lambda_k(A_n) = 1$ si $\pi(n)$ (le $(n + 1)$-ème nombre premier) divise k ;

$\lambda_k(A_n) = 0$ sinon.

Soient λ une distribution de valeur de vérité et c un entier. On trouve facilement un entier k tel que, pour tout $i \leqslant c$, $\lambda_k(A_i) = \lambda(A_i)$. Il suffit de prendre :

$$k = \prod_{0 < i < c} \pi(i)^{\lambda(A_i)},$$

et on voit que k peut être choisi inférieur ou égal à $\pi(c)!$.

Soit P une formule propositionnelle. On veut déterminer si P est une tautologie ou non. Il est d'abord clair que, si A_n est une variable propositionnelle apparaissant dans P, alors $n \leqslant \# P$. Il découle de tout ce qu'on vient de dire que P est une tautologie si et seulement si, pour tout entier k inférieur ou égal à $\pi(\# P)!$, $\lambda_k(P) = 1$. On commence donc par montrer :

LEMME : *La fonction* E *définie de la façon suivante :*

- si x *n'est pas le numéro de Gödel d'une proposition, alors*

$$E(k,x) = 0 \ ;$$

- si x *est le numéro de Gödel d'une proposition* P, *alors*

$$E(k,x) = \lambda_k(P) \ ;$$

est récursive primitive.

⊖ C'est encore le lemme 3.1 qui va nous tirer d'affaire. En effet, E peut se définir de la façon suivante :

- si $x \notin \text{Prop}$, alors $E(k,x) = 0$.
- sinon : - si $\beta_3^3(x) = 0$, alors :
  - si $\pi(\beta_3^1(x))$ divise k, alors $E(k,x) = 1$,
  - si $\pi(\beta_3^1(x))$ ne divise pas k, alors $E(k,x) = 0$;

- si $\beta_3^3(x) = 1$, alors $E(k,x) = 1 - E(k,\beta_3^1(x))$;
- si $\beta_3^3(x) = 2$, alors $E(k,x) = E(k,\beta_3^1(x)).E(k,\beta_3^2(x))$;
- si $\beta_3^3(x) = 3$, alors $E(k,x) = sg(E(k,\beta_3^1(x)) + E(k,\beta_3^2(x)))$;
- si $\beta_3^3(x) = 4$, alors $E(k,x) = sg(E(k,\beta_3^2(x)) + 1 - E(k,\beta_3^1(x)))$;
- si $\beta_3^3(x) = 5$, alors $E(k,x) = \begin{cases} 1 \text{ si } E(k,\beta_3^1(x)) = E(k,\beta_3^2(x)) ; \\ 0 \text{ sinon.} \end{cases}$

☺

Pour terminer la preuve du théorème, il suffit donc de remarquer que :

$$x \in \mathscr{T} \text{ si et seulement si } \forall k \leqslant \pi(x)!\ E(k,x) = 1.$$

☺

3.6 THEOREME : *L'ensemble :*

Taut = { # F ; F *est une formule et une tautologie du calcul des prédicats* }

est récursif primitif.

☺ A chaque formule F, on va faire correspondre une proposition P_F obtenue de la façon suivante : on écrit F sous la forme $P[F_1,F_2,...,F_k]$, où P est une proposition dont les variables propositionnelles sont $A_1,A_2,...,A_k$ et les formules $F_1,F_2,...,F_k$ ne peuvent pas être de nouveau décomposées à l'aide des connecteurs propositionnels, autrement dit, chaque formule F_i est : soit une formule atomique, soit une formule commençant par un quantificateur (pour une définition de la formule $P[F_1,F_2,...,F_k]$, voir chapitre 3, 1.22). Posons, pour chaque i, $\# F_i = c(i)$, puis :

$$P_F = P[A_{c(1)},A_{c(2)},...,A_{c(k)}].$$

Alors F est une tautologie du calcul des prédicats si et seulement si P_F est une tautologie : dans un sens (« si »), c'est simplement le lemme 3.5 du chapitre 3 ; pour l'autre (« seulement si »), on suppose que $F = J[G_1,G_2,...,G_m]$, où les G_j sont des formules du langage $\mathscr{L}_0$, et où $J[B_1,B_2,...,B_m]$ est une formule propositionnelle qui est une tautologie ; l'important est alors de remarquer qu'il y a évidemment une relation entre les formules propositionnelles J et P_F : précisément, P_F s'obtient à partir de J en y substituant aux variables propositionnelles B_1, B_2, ..., B_m, des formules propositionnelles adéquates, construites avec les variables $A_{c(1)}$, $A_{c(2)}$, ..., $A_{c(k)}$; sans donner de véritable preuve de cette affirmation, contentons-nous d'indiquer que la formule P_F représente en quelque sorte la décomposition propositionnelle maximale de F, que cette décomposition maximale est unique, au nom des variables propositionnelles près, et que la formule J représente, elle, un stade intermédiaire de la décomposition ; le fait que, si J est une tautologie du calcul propositionnel, alors P_F en est également une, résulte donc tout simplement du corollaire 2.8 du chapitre 1.

Il suffit donc de construire une fonction récursive primitive γ telle que, pour toute formule F, $\gamma(\# F) = \# P_F$. On aura alors :

$$x \in \text{Taut si et seulement si } x \in \text{Form et } \gamma(x) \in \mathcal{T}.$$

Comme d'habitude, on utilise le lemme 3.1 en définissant la fonction γ comme suit :

- Si $\beta_3^3(x) = 0$, 6 ou 7, alors $\gamma(x) = \alpha_3(x,0,0)$;
- si $\beta_3^3(x) = 1$, alors $\gamma(x) = \alpha_3(\gamma(\beta_3^1(x)),0,1)$;
- si $\beta_3^3(x) = 2,3,4$ ou 5, alors $\gamma(x) = \alpha_3(\gamma(\beta_3^1(x)),\gamma(\beta_3^2(x)),\beta_3^3(x))$;
- si $\beta_3^3(x) > 7$, alors on pose arbitrairement $\gamma(x) = 0$.

☺

3.7 On a maintenant tout ce qu'il faut pour montrer que les axiomes logiques forment un ensemble récursif primitif.

a) *L'ensemble :*

$$Ax_1 = \{\ \#(\exists v F \Longleftrightarrow \neg\forall v \neg F)\ ;\ F \textit{ est une formule et } v \textit{ est une variable}\ \}$$

est récursif primitif.

En effet, un calcul simple montre que :

$$\#(\exists v_n F \Longleftrightarrow \neg\forall v_n \neg F) = \alpha_3(\alpha_3(\# F,n,7),\alpha_3(\alpha_3(\alpha_3(\# F,0,1),n,6),0,1),5).$$

Donc, $x \in Ax_1$ si et seulement si il existe $y < x$ et $n < x$ tels que $y \in$ Form et

$$x = \alpha_3(\alpha_3(y,n,7),\alpha_3(\alpha_3(\alpha_3(y,0,1),n,6),0,1),5).$$

b) *L'ensemble :*

$Ax_2 = \{\ \#(\forall v(F \Longrightarrow G) \Longrightarrow (F \Longrightarrow \forall v G))\ ;\ F$ *et* G *sont des formules et* v *est une variable qui n'a pas d'occurrence libre dans* F $\}$

est récursif primitif.

Même chose : $x \in Ax_2$ si et seulement si il existe y, z et n inférieurs à x tels que $(y,n) \in \Phi_1$ (voir 3.4), $z \in$ Form et :

$$x = \alpha_3(\alpha_3(\alpha_3(y,z,4),n,6),\alpha_3(y,\alpha_3(z,n,6),4),4).$$

c) *L'ensemble :*

$Ax_3 = \{\ \#(\forall v F \Longrightarrow F_{t/v})$; v *est une variable,* F *est une formule,* t *est un terme et, dans* F, *aucune occurrence libre de* v *ne se trouve dans le champ d'un quantificateur liant une variable de* t $\}$

est récursif primitif.

Il faut d'abord se persuader que l'ensemble :

$B = \{\ (\# F,n,m)$; aucune occurrence libre de v_m dans F ne se trouve dans le champ d'un quantificateur $\forall v_n$ ou $\exists v_n$ $\}$

est récursif primitif. Cela se fait, comme d'habitude, en utilisant le lemme 3.1. La

fonction caractéristique g de B peut être définie de la façon suivante :

- si $x \notin$ Form, alors $g(x,n,m)=0$;
- si $x \in$ Form, alors :
  - si $\beta_3^3(x)=0$, alors $g(x,n,m)=1$;
  - si $\beta_3^3(x)=1$, alors $g(x,n,m)=g(\beta_3^1(x),n,m)$;
  - si $\beta_3^3(x) \in \{2,3,4,5\}$, alors $g(x,n,m)=g(\beta_3^1(x),n,m)\cdot g(\beta_3^2(x),n,m)$;
  - si $\beta_3^3(x) \in \{6,7\}$, alors,
    - si $\beta_3^2(x)=n$ et $(\beta_3^1(x),m) \in \Phi_4$ (voir 3.4), alors $g(x,n,m)=0$;
    - sinon, $g(x,n,m)=g(\beta_3^1(x),n,m))$.

Ensuite, il suffit de traduire : $x \in Ax_3$ si et seulement si il existe y, z et m inférieurs à x tels que $y \in$ Form, $z \in$ Term, pour tout $n < z$, $((z,n) \in \Theta_0$ ou $(y,n,m) \in B)$ et :

$$x=\alpha_3(\alpha_3(y,m,6),\mathrm{subs_f}(m,z,y),4).$$

De tout cela il découle :

THEOREME : *L'ensemble* $Ax=\{\#F \ ; \ F$ *est un axiome logique*$\}$ *est récursif primitif.*

3.8 DEFINITIONS :

1) Soit T *une théorie ; on dit que* T *est* ***récursive*** *si l'ensemble :*

$$\#T=\{\#F \ ; F\in T\}$$

est récursif.

2) On notera $Th(T)=\{\#F \ ; F$ *est une formule close et* $T\vdash F\}$ *(*$Th(T)$ *est l'ensemble des numéros de Gödel des théorèmes de* T*).*

3) On dit que T *est* ***décidable*** *si* Th(T) *est récursif. Une théorie* ***indécidable*** *est une théorie qui n'est pas décidable.*

REMARQUE : Etre récursive, pour une théorie, est une condition raisonnable ; on peut même dire que ce sont les théories non récursives qui sont artificielles : comment peut-on espérer faire une démonstration si on ne connaît pas effectivement les axiomes ? En revanche, on va voir que beaucoup de théories naturelles et intéressantes ne sont pas décidables.

EXEMPLE : La théorie vide est récursive ; l'ensemble de ses théorèmes est tout simplement l'ensemble des formules closes valides. Les théories finies comme $\mathscr{P}_0$ sont aussi récursives. Il n'est pas difficile de voir que $\mathscr{P}$ est récursive.

NOTATION : Soit $d = (F_0, F_1, \ldots, F_k)$ une suite de formules du langage $\mathscr{L}_0$; par ##d , on désignera l'entier :

$$\#\#d = \Omega((\#F_0, \#F_1, \ldots, \#F_k))$$

(encore une fois, Ω est la fonction introduite au chapitre 5, en 1.12).
On appellera encore **numéro de Gödel de** d l'entier ##d.

PROPOSITION : *Soit* T *une théorie récursive ; alors l'ensemble :*

$$\mathrm{Dem}(T) = \{ (n,m) \; ; \; n = \#F, \; m = \#\#d, \; F \textit{ est une formule et } d \textit{ est une démonstration de } F \textit{ à partir de } T \}$$

est récursif.

☹ Il suffit de se reporter à la définition d'une démonstration (chapitre 4, 1.3) et de se rendre compte que le procédé permettant de vérifier si une suite de formules est une démonstration est effectif :

$(n,m) \in \mathrm{Dem}(T)$ si et seulement si les trois conditions suivantes sont vérifiées :

1) pour tout $i < \lg(m)$, $\delta(i,m) \in \mathrm{Form}$;
2) $\delta(\lg(m) - 1, m) = n$;
3) pour tout $i < \lg(m)$, $\delta(i,m) \in \mathrm{Ax} \cup \#T$, ou bien il existe $j < i$ et $p < m$ tels que $\delta(i,m) = \alpha_3(\delta(j,m),p,6)$, ou bien il existe $j < i$ et $k < i$ tels que $\delta(j,m) = \alpha_3(\delta(k,m),\delta(i,m),4)$.

(où $\lg(m)$ désigne la longueur du mot codé par m.)
La clause 3) exprime que chaque formule de la démonstration est, soit un axiome (si $\delta(i,m) \in \mathrm{Ax} \cup \#T$), soit une formule déduite par généralisation d'une formule déjà démontrée (s'il existe $j < i$ et $p < m$ tels que $\delta(i,m) = \alpha_3(\delta(j,m),p,6)$), soit une formule déduite par modus ponens de deux formules déjà démontrées (s'il existe $j < i$ et $k < i$ tels que $\delta(j,m) = \alpha_3(\delta(k,m),\delta(i,m),4)$)).
☺

COROLLAIRE : *Soit* T *une théorie récursive ; alors* Th(T) *est récursivement énumérable. En particulier, les ensembles suivants sont récursivement énumérables :*

- { #F ; F *est une formule close valide* } ;
- { #F ; F *est un théorème de* $\mathscr{P}_0$ } ;
- { #F ; F *est un théorème de* $\mathscr{P}$ }.

☹ En effet, $n \in Th(T)$ si et seulement si $n \in \Phi_3$ et il existe un entier m tel que $(n,m) \in Dem(T)$; $Th(T)$ est donc l'intersection d'un ensemble récursif avec la projection d'un ensemble récursif, et est donc récursivement énumérable (voir chapitre 5, 4.3).
☺

3.9 Concluons par un autre corollaire :

COROLLAIRE : *Si* T *est une théorie complète et récursive, alors elle est décidable.*

☹ On sait déjà que $Th(T)$ est un ensemble récursivement énumérable ; on va montrer que son complémentaire l'est aussi, et on pourra conclure par le théorème 4.2 du chapitre 5. Parce que T est complète, si F est une formule close qui n'est pas un théorème de T, alors $\neg F$ est un théorème de T, ce qui se traduit par :

$$m \notin Th(T) \text{ si et seulement si } m \notin \Phi_3 \text{ ou } \alpha_3(m,0,1) \in Th(T).$$

☺

4. LES THEOREMES D'INCOMPLETUDE ET D'INDECIDABILITE

Indécidabilité de l'arithmétique et du calcul des prédicats

4.1 Les derniers corollaires de la section précédente laissent béantes les questions suivantes : la théorie vide est-elle décidable ? $\mathscr{P}_0$ est-elle décidable ? et $\mathscr{P}$? Dans cette section, on va voir que, les trois fois, la réponse est non et montrer les théorèmes les plus célèbres de la logique mathématique.

Dans toute cette section, les théories considérées sont exprimées dans un langage fini contenant $\mathscr{L}_0$ (voir les remarques introductives à la section 3).

THEOREME : *Soit* T *une théorie cohérente contenant* $\mathscr{P}_0$; *alors* T *est indécidable.*

☹ On va supposer que T est une théorie décidable contenant $\mathscr{P}_0$ et on va construire une formule close F de $\mathscr{L}_0$ telle que $T \vdash F$ et $T \vdash \neg F$. On va se servir pour cela de la section 2 sur la représentation des fonctions récursives.

Considérons l'ensemble :

$\Theta = \{ (m,n)$; m est le numéro de Gödel d'une formule $F[v_0]$ dont v_0 est la seule variable libre éventuelle et $T \vdash F[\underline{n}] \}$.

Il est d'abord clair que, puisque T est décidable, Θ est récursif : en effet, l'ensemble A des numéros de Gödel des formules dont v_0 est la seule variable libre éventuelle est certainement récursif : $m \in A$ si et seulement si, pour tout p compris entre 1 et m, $(m,p) \notin \Phi_4$ (voir 3.4, lemme 1). La fonction $\lambda n.\#\underline{n}$ est aussi récursive : elle se définit par récurrence par : $\#\underline{0} = \alpha_3(0,0,0)$, et $\#(\underline{n+1}) = \alpha_3(\#\underline{n},0,1)$. On voit alors que :

$$(m,n) \in \Theta \text{ si et seulement si } m \in A \text{ et } \mathrm{Subs}_f(0,\#\underline{n},m) \in \mathrm{Th}(T).$$

Il en résulte que l'ensemble :

$$B = \{ n \in \mathbb{N} \; ; (n,n) \notin \Theta \}$$

est aussi récursif, et, d'après le théorème de représentation (2.2), il existe une formule $G[v_0]$ qui le représente. On a donc, pour tout $n \in \mathbb{N}$:

(*) $n \in B$ implique $\mathscr{P}_0 \vdash G[\underline{n}]$, donc $T \vdash G[\underline{n}]$;

(**) $n \notin B$ implique $\mathscr{P}_0 \vdash \neg G[\underline{n}]$, donc $T \vdash \neg G[\underline{n}]$.

Par ailleurs, $\#G[v_0]$ est un entier appartenant à A que nous appellerons a. On voit d'abord qu'il est impossible que a appartienne à B : par définition de B, cela impliquerait que $(a,a) \notin \Theta$, et par définition de Θ, qu'il est faux que $T \vdash G[\underline{a}]$, et ceci contredit l'assertion (*) ci-dessus. Il faut donc en déduire que $a \notin B$ et que $(a,a) \in \Theta$. D'une part, par définition de Θ on a $T \vdash G[\underline{a}]$; d'autre part, (**) implique $T \vdash \neg G[\underline{a}]$: T n'est pas cohérente.

☺

4.2 Le corollaire suivant est le **théorème de Church**. Il montre l'**indécidabilité du calcul des prédicats**.

COROLLAIRE : *La théorie :*

$T_0 = \{$ F ; F *est une formule close de* $\mathscr{L}$ *universellement valide* $\}$

n'est pas récursive.

☹ Soit G la conjonction de tous les axiomes de $\mathscr{P}_0$ (c'est ici qu'on se félicite d'avoir travaillé avec une théorie finie !). Il est alors clair que, pour toute formule close F de $\mathscr{L}_0$,

$$\mathscr{P}_0 \vdash F \text{ si et seulement si } (G \Longrightarrow F) \in T_0.$$

On voit donc que, si T_0 était récursive, $\mathscr{P}_0$ serait décidable, ce qui n'est pas vrai, d'après le théorème précédent.

☺

REMARQUES : L'énoncé du dernier corollaire n'a de sens que si l'on a arithmétisé la syntaxe de $\mathscr{L}$, mais sa démonstration est indépendante de cette arithmétisation, dès lors qu'elle prolonge celle que nous avons détaillée sur $\mathscr{L}_0$.

L'indécidabilité du calcul des prédicats a été démontrée seulement pour les langages contenant le langage de l'arithmétique. On verra dans l'exercice 11 qu'il suffit de supposer que le langage contienne un symbole de prédicat binaire. Mais le théorème est faux pour les langages trop pauvres ne contenant que des symboles de prédicats unaires.

Les théorèmes d'incomplétude de Gödel

4.3 Voici maintenant le **premier théorème d'incomplétude** (de **Gödel–Rosser**) :

THEOREME : *Soit* T *une théorie récursive et cohérente contenant* $\mathscr{P}_0$. *Alors* T *n'est pas complète. En particulier* $\mathscr{P}$ *n'est pas complète.*

☹ Avec ce que l'on sait déjà (théorème 4.1), il suffit de se rappeler qu'une théorie récursive et complète est décidable (corollaire 3.9).

☺

Il y a donc des formules closes de $\mathscr{L}_0$ qui ne sont ni démontrées ni réfutées par les axiomes de Peano. En suivant la démonstration du théorème d'incomplétude, on arriverait, si on le désirait, à construire une telle formule. Mais cela ne nous dirait pas si cette formule a une signification, ni, le cas échéant, laquelle.

Le second théorème d'incomplétude de Gödel répond à cette question de façon frappante : c'est une formule exprimant que les axiomes de Peano sont cohérents. Cette formule est vérifiée dans le modèle standard, mais comme elle n'est pas démontrable, d'après le théorème de complétude du chapitre 4, il y a des modèles des axiomes de Peano dans lesquels elle est fausse.

4.4 L'énoncé même du second théorème d'incomplétude demande quelques notations et un peu de travail. Soit T une théorie récursive contenant $\mathscr{P}$; considérons les deux ensembles récursifs Dem et Dem_0 définis par :

Dem = { (a,b) ; a est le numéro de Gödel d'une formule close F et b est le numéro de Gödel d'une démonstration de F dans T } ;

Dem_0 = { (a,b) ; a est le numéro de Gödel d'une formule close F et b est le numéro de Gödel d'une démonstration de F dans $\mathscr{P}_0$ }.

D'après le théorème de représentation, il existe deux formules du langage de l'arithmétique à deux variables libres qui représentent ces ensembles. On va choisir deux telles formules que l'on notera $\mathfrak{Dem}$ et $\mathfrak{Dem}_0$ respectivement (on reviendra plus loin sur la façon de faire ce choix). La cohérence de la théorie T peut alors s'exprimer par une formule de $\mathscr{L}_0$. Il suffit de dire qu'on ne peut pas démontrer quelque chose et son contraire. Définissons pour cela la fonction récursive primitive Neg de $\mathbb{N}$ dans $\mathbb{N}$ par :

• si n est le numéro de Gödel d'une formule close F, alors Neg(n) est le numéro de Gödel de ¬F, c'est-à-dire $\mathrm{Neg}(n) = \alpha_3(n,0,1)$;

• sinon, $\mathrm{Neg}(n) = 0$.

Soit $\mathfrak{Neg}[v_0,v_1]$ une formule représentant cette fonction. La formule Coh(T) est par définition la formule :

$$\mathrm{Coh(T)} = \neg\exists v_0\exists v_1\exists v_2\exists v_3(\mathfrak{Dem}[v_0,v_2] \wedge \mathfrak{Dem}[v_1,v_3] \wedge \mathfrak{Neg}[v_0,v_1])$$

La formule Coh(T) mérite bien son nom : supposons que la théorie T ne soit pas cohérente ; alors il existe une formule close F et deux démonstrations formelles d_0 et d_1, respectivement de F et de ¬F. Si n_0 ,n_1 ,m_0 et m_1 sont les numéros de Gödel respectifs de F, ¬F, d_0 et d_1, alors on voit que :

$$\mathbb{N} \models \mathfrak{Dem}[n_0,m_0] \wedge \mathfrak{Dem}[n_1,m_1] \wedge \mathfrak{Neg}[n_0,n_1],$$

et donc :

$$\mathbb{N} \models \neg\mathrm{Coh(T)}.$$

Réciproquement, si :

$$\mathbb{N} \models \neg\mathrm{Coh(T)},$$

alors on peut trouver des entiers n_0 ,n_1 ,m_0 et m_1 tels que :

$$\mathbb{N} \models \mathfrak{Dem}[n_0,m_0] \wedge \mathfrak{Dem}[n_1,m_1] \wedge \mathfrak{Neg}[n_0,n_1],$$

et donc $(n_0,m_0) \in$ Dem, $(n_1,m_1) \in$ Dem et $(n_0,n_1) \in$ Neg : n_0 est le numéro de Gödel d'une formule qui est démontrable, ainsi que sa négation.

On va voir qu'il est toutefois possible d'avoir un modèle $\mathfrak{M}$ de $\mathscr{P}$ dans lequel la formule ¬Coh(T) est vérifiée, bien que la théorie T soit cohérente. Cela veut tout simplement dire qu'il existe des éléments a_0 ,a_1, a_2, a_3 dans $\mathfrak{M}$ tels que :

$$\mathfrak{M} \models \mathfrak{Dem}[a_0,a_2] \wedge \mathfrak{Dem}[a_1,a_3] \wedge \mathfrak{Neg}[a_0,a_1] ;$$

le fait que a_1, a_2, a_3 et a_4 ne sont pas nécessairement des entiers standard nous empêche d'aller plus loin et de conclure, comme dans le cas de $\mathbb{N}$, à la non cohérence de T.

Cependant, dans tout modèle de $\mathscr{P}$, les formules $\mathfrak{Dem}$ et $\mathfrak{Neg}$ continuent à avoir certaines propriétés auxquelles nous sommes habitués. Par exemple, un fait qui découle formellement de la façon dont Coh(T) a été définie et dont on se servira par la suite est le suivant : supposons que $b \in \mathbb{N}$ soit le numéro de Gödel d'une formule close F et que d soit le numéro de Gödel de ¬F (c'est-à-dire $d = \alpha_3(b,0,1)$) . Alors :

$$\mathscr{P}_0 \vdash (\exists v_0 \mathfrak{Dem}[\underline{b},v_0] \wedge \exists v_1 \mathfrak{Dem}[\underline{d},v_1]) \Longrightarrow \neg \mathrm{Coh}(T)).$$

4.5 Nous sommes maintenant en mesure d'énoncer **le second théorème d'incomplétude de Gödel** :

THEOREME : *Soit* T *une théorie cohérente, récursive et contenant* $\mathscr{P}$. *Alors* T *ne démontre pas* Coh(T).

Il faut toutefois être un peu prudent. En effet, si les ensembles Dem et Dem_0 sont parfaitement définis, on a déjà remarqué qu'il n'en était pas de même des formules $\mathfrak{Dem}$ et $\mathfrak{Dem}_0$, et, par voie de conséquence, de la formule Coh(T). La seule chose que nous sachions, a priori, sur ces formules est qu'elles représentent les ensembles Dem et Dem_0 ; on connaît exactement les entiers qui les vérifient, mais on ne sait pas grand chose de leur comportement en dehors des éléments standards ; de fait, on peut trouver (voir exercice 8) deux formules $D[v_0,v_1]$ et $D'[v_0,v_1]$ qui, toutes deux, représentent Dem_0, mais qui ne sont pas équivalentes, dans le sens où $\mathscr{P}$ ne démontre pas la formule :

$$\forall v_0 \forall v_1 (D[v_0,v_1] \Longleftrightarrow D'[v_0,v_1]).$$

Comme on a besoin de la formule $\mathfrak{Dem}$ pour énoncer le second théorème d'incomplétude (pour écrire Coh(T)), il faut bien savoir à laquelle on a affaire.

Pour résumer, le théorème d'incomplétude énoncé ci-dessus n'est vrai que si on a fait le bon choix pour la formule $\mathfrak{Dem}$, et il semblerait bien qu'il faille se résoudre à l'écrire effectivement. Cela pourrait se faire, en la construisant pas à pas et en suivant la preuve du théorème de représentation et la preuve du fait que l'ensemble Dem est récursif. On obtiendrait ainsi une formule $\mathfrak{Dem}$ plus ou moins canonique, dans le sens (approximatif) suivant : si deux personnes de bonne foi faisaient cette construction, elles tomberaient sûrement sur deux formules équivalentes modulo $\mathscr{P}$. Mais ce n'est pas ce que l'on fera, car cela exigerait des écritures et des vérifications beaucoup trop longues et ennuyeuses. Il est plus facile d'isoler les propriétés, peu nombreuses en fait, que doivent vérifier ces formules pour permettre la preuve du second théorème d'incomplétude. On verra ensuite comment se débrouiller avec ces propriétés.

4.6 Pour cela, nous avons besoin d'une définition :

DEFINITION : *L'ensemble Σ est le plus petit ensemble de formules du langage $\mathscr{L}_0$ qui :*

i) contient toutes les formules sans quantificateur ;

ii) est clos par conjonction et disjonction (si F *et* G *sont dans Σ, il en est de même de* $F \wedge G$ *et de* $F \vee G$) ;

iii) est clos par quantification existentielle ;

iv) est clos par quantification universelle bornée (si F *est dans Σ, alors* $\forall v_0(v_0 < v_1 \Longrightarrow F)$, *qu'on écrira* $(\forall v_0 < v_1)\ F$, *est aussi dans Σ).*

On dira qu'une formule F ***est sigma*** *(on écrira : « F est Σ ») si* F *appartient à Σ.*

(Remarque : cet ensemble fait partie d'une célèbre famille et est en général appelé Σ_1^0 (lire « sigma zéro un ») ; comme c'est le seul membre de cette famille qui sera considéré ici, on ne s'embarrassera pas d'indices.)

Par exemple, on peut voir sans difficulté que les relations « n divise m » ou « n est un nombre premier » s'expriment par des formules Σ. Il faut prendre garde cependant au fait que l'ensemble Σ n'est pas clos par négation.

Voici les propriétés que l'on exige des formules $\mathfrak{Dem}$ et $\mathfrak{Dem}_0$:

(P_1) $\vdash \forall v_0 \forall v_1(\mathfrak{Dem}_0[v_0,v_1] \Longrightarrow \mathfrak{Dem}[v_0,v_1])$;

(P_2) $\mathfrak{Dem}$ et $\mathfrak{Dem}_0$ sont des formules Σ ;

(P_3) si F est une formule close Σ, alors $\mathscr{P} \vdash F \Longrightarrow \exists v_1 \mathfrak{Dem}_0[\underline{\#F},v_1]$.

La première n'est pas très difficile à justifier. Elle est on ne peut plus naturelle puisque T contient $\mathscr{P}_0$. De toute façon, si la propriété (P_1) n'était pas vérifiée, il suffirait de remplacer $\mathfrak{Dem}[v_0,v_1]$ par $\mathfrak{Dem}[v_0,v_1] \vee \mathfrak{Dem}_0[v_0,v_1]$.

Pour la seconde, il suffit de reprendre la preuve du théorème de représentation ; on s'aperçoit en fait que cette même preuve donne un **théorème de représentation bis** :

THEOREME : *Toute fonction récursive totale est représentable par une formule Σ.*

En conséquence, on supposera que les formules $\mathfrak{Dem}$, $\mathfrak{Dem}_0$ et toutes les formules dont on peut avoir besoin pour représenter un ensemble ou une fonction récursive sont Σ. Voici un autre résultat qui donne de l'importance aux formules Σ et un début de justification à (P_3) :

PROPOSITION : *Soit* F *une formule close* Σ *de* $\mathscr{L}_0$. *Alors :*

$$\mathbb{N} \models F \Longrightarrow \exists v_1 \mathfrak{Dem}_0[\underline{\#F}, v_1].$$

(Autrement dit, si F est une formule close Σ, $\mathbb{N} \models F$ si et seulement si $\mathscr{P}_0 \vdash F$.)

☺ Si F est fausse dans $\mathbb{N}$, évidemment, la formule $F \Longrightarrow \exists v_1 \mathfrak{Dem}_0[\underline{\#F}, v_1]$ y est vraie. Si elle est vraie, on va montrer qu'elle est démontrable dans $\mathscr{P}_0$, et pour cela, on va utiliser le théorème de complétude : il suffit de voir que F est vraie dans n'importe quel modèle de $\mathscr{P}_0$. Mais tout modèle de $\mathscr{P}_0$ peut être considéré comme une extension finale de $\mathbb{N}$ (théorème 1.6). Le lemme suivant terminera donc la preuve :

LEMME : *Soit* $\mathfrak{N}$ *une* $\mathscr{L}_0$*-structure,* $\mathfrak{M}$ *une extension finale de* $\mathfrak{N}$, $F[v_1,v_2,\ldots v_p]$ *une formule* Σ *et* $a_1,a_2,\ldots,a_p$ *des points de* $\mathfrak{N}$. *Alors :*

$$\mathfrak{N} \models F[a_1,a_2,\ldots,a_p] \quad \textit{implique} \quad \mathfrak{M} \models F[a_1,a_2,\ldots,a_p].$$

☺ On raisonne par induction. On considère l'ensemble des formules G qui sont telles que, pour tous $a_1,a_2,\ldots,a_p$ de $\mathfrak{N}$ (p étant le nombre de variables libres de G) :

$$\mathfrak{N} \models G[a_1,a_2,\ldots,a_p] \quad \text{implique} \quad \mathfrak{M} \models G[a_1,a_2,\ldots,a_p].$$

On voit facilement que cet ensemble contient toutes les formules sans quantificateur et est clos par conjonction et disjonction ; il est aussi clos par quantification existentielle parce que $\mathfrak{N}$ est une sous-structure de $\mathfrak{M}$, et il est clos par quantification universelle bornée parce que $\mathfrak{M}$ est une extension finale de $\mathfrak{N}$. Cet ensemble contient donc toutes les formules Σ.

☺

☺

4.7 Posons :

$$\mathscr{P}_1 = \mathscr{P}_0 \cup \{ F \Longrightarrow \exists v_1 \mathfrak{Dem}_0[\underline{\#F}, v_1] \text{ ; F est une formule } \Sigma \text{ close } \}.$$

On vient de voir que $\mathbb{N}$ est un modèle de $\mathscr{P}_1$. Il découle aussi facilement de tous les lemmes que l'on a démontrés à la section 3 que $\mathscr{P}_1$ est une théorie récursive. Le second théorème d'incomplétude se déduit alors des deux lemmes suivants :

LEMME 1 : *Toute formule de $\mathscr{P}_1$ est conséquence de $\mathscr{P}$.*

LEMME 2 : *Soit* T *une théorie récursive cohérente qui démontre toutes les formules de $\mathscr{P}_1$. Alors* T *ne démontre pas* Coh(T).

Remarquons que le lemme 2 implique immédiatement qu'une théorie récursive cohérente qui contient $\mathscr{P} \cup \mathscr{P}_1$ ne démontre pas sa propre cohérence, ce qui constitue déjà une bonne approximation du second théorème d'incomplétude. (On peut montrer que $\mathscr{P}_1$, qui est syntaxiquement plus simple que $\mathscr{P}$, est en fait bien plus faible que $\mathscr{P}$; par conséquent, le lemme 2 donne une version forte du second théorème d'incomplétude). La preuve de lemme 2, on va le voir, n'est pas trop difficile. La preuve du lemme 1 n'est pas très difficile non plus, mais elle est longue et ennuyeuse. Elle exige un grand nombre de vérifications fastidieuses. On va donc laisser le choix au lecteur : s'il insiste pour avoir la preuve complète, il faudra qu'il démontre le lemme 1 par lui-même ; on se bornera ici à donner quelques indications sur cette démonstration. Sinon, soit que notre lecteur admette le lemme 1, soit qu'il se contente d'une forme légèrement affaiblie du théorème, on lui donne rendez-vous quelques lignes plus loin pour la démonstration du lemme 2.

4.8 **Indications pour la preuve du lemme 1** :

☹ Une mise en garde avant tout ; voici l'énoncé exact du lemme 1 : il existe une formule $\mathfrak{Dem}_0[v_0,v_1]$ de $\mathscr{L}_0$ qui est Σ, qui représente l'ensemble Dem_0 et qui est telle que, pour toute formule sigma F de $\mathscr{L}_0$, on ait :

$$\mathscr{P} \vdash F \Longrightarrow \exists v_1 \mathfrak{Dem}_0[\underline{\#F}, v_1].$$

L'idée qui va nous servir de fil conducteur est simple : on reprend l'argument qui nous a permis d'affirmer que pour toute formule F qui est close et Σ,

$$\mathbb{N} \models F \Longrightarrow \exists v_1 \mathfrak{Dem}_0[\underline{\#F}, v_1],$$

et on va le formaliser dans $\mathscr{P}$.

Voici quelques rappels et remarques avant de s'engager dans cette voie : soient $n \in \mathbb{N}$ et $\mathfrak{M}$ un modèle de $\mathscr{P}$. Appelons M l'ensemble sous-jacent à $\mathfrak{M}$. Un sous-ensemble X de M^n est définissable s'il existe une formule $F[v_0,v_1,\dots,v_{n-1}]$ de L telle que :

$$X = \{ (a_0,a_1,\dots,a_{n-1}) \in M^n ; \mathfrak{M} \models F[a_0,a_1,\dots,a_{n-1}] \}.$$

Une application de M^n dans M est définissable si son graphe l'est ; un élément a est définissable si $\{ a \}$ est définissable.

Si $F[v_0,v_1,\dots,v_n]$ est une formule de $\mathscr{L}_0$, le fait que, dans tout modèle de $\mathscr{P}$, l'ensemble défini par F est le graphe d'une application de $\mathbb{N}^n$ dans $\mathbb{N}$ s'exprime par :

$$\mathscr{P} \vdash \forall v_1 \forall v_2 \dots \forall v_n \exists! v_0 F[v_0,v_1,\dots,v_n].$$

La formule $\forall v_1 \forall v_2 \dots \forall v_n \exists! v_0 F[v_0,v_1,\dots,v_n]$ sera désignée par l'écriture : « F **définit une**

application de M^n dans M ». On fera de même pour d'autres propriétés s'exprimant par des formules de $\mathcal{L}_0$: l'énoncé de la propriété écrit entre guillemets représentera la (ou plutôt une) formule qui l'exprime.

Les raisonnements par récurrence nous sont permis puisque le schéma SI est inclus dans $\mathcal{P}$. On peut aussi définir des applications par récurrence. Très exactement :

Soient F *et* G *des formules de* $\mathcal{L}_0$, n *un entier et supposons que :*
$\mathcal{P} \vdash$ « F définit une application de M^n dans M » $\wedge$ « G définit une application de M^{n+2} dans M ».
Alors, pour tout modèle $\mathfrak{M}$ *de* $\mathcal{P}$, *si on appelle* f *et* g *les fonctions définies respectivement par* F *et* G *dans* $\mathfrak{M}$, *alors il existe une et une seule fonction définissable* h *de* M^{n+1} *dans* M *telle que :*
- *pour tous éléments* $a_1, a_2, \ldots, a_n$ *de* M, $h(0,a_1,a_2,\ldots,a_n) = f(a_1,a_2,\ldots,a_n)$;
- *pour tous éléments* $a_0, a_1, \ldots, a_n$ *de* M, $h(a_0+1,a_1,\ldots,a_n) = g(a_0,a_1,\ldots,a_n,h(a_0,a_1,\ldots,a_n))$.

Cette fonction est définie par une formule H *dépendant récursivement de* F *et* G *(mais pas de* $\mathfrak{M}$*). De plus, si* F *et* G *sont des formules* Σ, *alors* H *peut aussi être choisie* Σ.

On établit ce résultat en démontrant d'abord dans $\mathcal{P}$ quelques faits simples d'arithmétique, afin de pouvoir généraliser le lemme 4 de 2.3.

On peut alors construire des formules Σ : « v_0 est le code d'une formule close de $\mathcal{L}_0$ », « v_0 est le code d'une formule de $\mathcal{L}_0$ ayant une seule variable libre », « v_0 est le code d'une formule close de $\mathcal{L}_0$ et v_1 est le code d'une démonstration de celle-ci », etc. L'avantage de ces formules par rapport à celles que l'on obtiendrait en appliquant le théorème de représentation, c'est qu'un certain nombre de faits concernant la propriété écrite entre guillemets se traduisent par des théorèmes de $\mathcal{P}$. Par exemple le lemme de déduction (chapitre 4, 1.7) et la proposition 2.4 du chapitre 4.

Il reste le plus difficile, qui est le théorème de complétude. On se bornera au langage $\mathcal{L}_0$. Etant donnée une suite de cinq formules $\mathcal{H} = (H_0[v_0],H_1[v_0],H_2[v_0,v_1], H_3[v_0,v_1,v_2],H_4[v_0,v_1,v_2])$, on peut facilement trouver une formule close G (dépendant récursivement de $\mathcal{H}$) qui exprime que, dans tout modèle de $\mathcal{P}$: l'ensemble X_0 défini par H_0 n'est pas vide, que l'ensemble défini par H_1 est réduit à un élément a qui appartient à X_0, H_2 définit une fonction de X_0 dans lui-même, H_3 et H_4 définissent des fonctions de $X_0 \times X_0$ dans X_0. Si $\mathcal{H}$ satisfait ces conditions et si $\mathfrak{M}$ est un modèle de $\mathcal{P}$, alors on appellera $\mathfrak{M}(\mathcal{H})$ la $\mathcal{L}_0$-structure dont l'ensemble de base est $\{a \in M ; \mathfrak{M} \models H_0[a]\}$, où l'interprétation de $\underline{0}$ est l'unique élément de M vérifiant H_1, et où les interprétations de $\underline{S}$, $\underline{+}$ et $\underline{\times}$ sont les fonctions définies dans $\mathfrak{M}$ par H_2, H_3 et H_4. Etant données une suite $\mathcal{H}$ comme ci-dessus et une formule $F[v_0,v_1,\ldots,v_k]$ de $\mathcal{L}_0$, on peut, par récurrence ordinaire sur la hauteur de F (voir aussi l'exercice 11), construire une formule de $\mathcal{L}_0$ que l'on notera « $(v_0,v_1,\ldots,v_k)$ satisfait la formule F dans $\mathfrak{M}(\mathcal{H})$ » et qui est telle que : pour tout modèle $\mathfrak{M}$ de $\mathcal{P}$, pour tous éléments $a_0, a_1,\ldots, a_k$ de M vérifiant H_0, on a :

$\mathfrak{M}(\mathscr{H}) \models F[a_0,a_1,\dots,a_k]$ si et seulement si

$\mathfrak{M} \models$ « $(a_0,a_1,\dots,a_k)$ satisfait la formule F dans $\mathfrak{M}(\mathscr{H})$ ».

La formule « $(v_0,v_1,\dots,v_k)$ satisfait la formule F dans $\mathfrak{M}(\mathscr{H})$ » dépend récursivement de F et de $\mathscr{H}$.

On peut maintenant énoncer la version du **théorème de complétude dans Peano** :

Pour toute formule close F, *il existe une suite de cinq formules* $\mathscr{H} = (H_0[v_0], H_1[v_0], H_2[v_0,v_1], H_3[v_0,v_1,v_2], H_4[v_0,v_1,v_2])$ *(dépendant récursivement de* F*) telle que :*

$$\mathscr{P} \vdash \text{Coh(F)} \Longrightarrow \text{« F est vérifiée dans } \mathfrak{M}(\mathscr{H}) \text{ »}.$$

(Ici, Coh(F) est la formule : $\neg\exists v_0$(« v_0 est le code d'une démonstration de $\neg$F ») et « F est vérifiée dans $\mathfrak{M}(\mathscr{H})$ » est la formule « la suite vide satisfait la formule F dans $\mathfrak{M}(\mathscr{H})$ ».)

La preuve de ce théorème se fait en suivant la preuve du théorème de complétude (voir chapitre 4, 2.6). Nous n'insisterons pas sur ce point.

On termine maintenant la preuve du lemme 1 : la formule $\mathfrak{Dem}_0[v_0,v_1]$ est la formule « v_0 est le code d'une formule close de $\mathscr{L}_0$ et v_1 est le code d'une démonstration de celle-ci dans $\mathscr{P}_0$ ». Pour montrer que, si F est une formule close Σ, alors on a : $\mathscr{P} \vdash F \Longrightarrow \exists v_1 \mathfrak{Dem}_0[\underline{\#F}, v_1]$, on utilise le théorème de complétude ordinaire : on montre que la formule $F \Longrightarrow \exists v_1 \mathfrak{Dem}_0[\underline{\#F}, v_1]$ est vraie dans tout modèle de $\mathscr{P}$. Considérons un modèle $\mathfrak{M} = \langle M, 0, S, +, \times \rangle$ de $\mathscr{P}$. Si $\exists v_1 \mathfrak{Dem}_0[\underline{\#F}, v_1]$ est vraie dans $\mathfrak{M}$, alors la formule $F \Longrightarrow \exists v_1 \mathfrak{Dem}_0[\underline{\#F}, v_1]$ y est vraie aussi. Sinon, appelons G la conjonction des formules de $\mathscr{P}_0$ et de $\neg$F. La formule $\neg\exists v_1 \mathfrak{Dem}_0[\underline{\#F}, v_1]$ est équivalente à Coh(G), et donc :

$$\mathfrak{M} \models \text{Coh(G)}.$$

On applique alors la version du théorème de complétude dans Peano : il existe une suite de cinq formules $\mathscr{H}$ comme ci-dessus définissant une $\mathscr{L}_0$-structure :

$$\mathfrak{M}(\mathscr{H}) = \langle X, 0', S', +', \times' \rangle,$$

telle que :

$\mathfrak{M} \models$ « G est vérifiée dans $\mathfrak{M}(\mathscr{H})$ »,

et donc $\mathfrak{M}(\mathscr{H}) \models G$.

On peut définir par récurrence dans $\mathfrak{M}$ une application définissable k de M dans X par : $k(0) = 0'$ et, pour tout $a \in M$, $k(S(a)) = S'(k(a))$. On montre que k est un monomorphisme de $\mathfrak{M}$ dans $\mathfrak{M}(\mathscr{H})$, et que l'image de k est un segment initial de $\mathfrak{M}(\mathscr{H})$ (il faut utiliser le schéma d'induction dans $\mathfrak{M}$ et le fait que $\mathfrak{M}(\mathscr{H})$ est modèle de $\mathscr{P}_0$). La structure $\mathfrak{M}(\mathscr{H})$ est donc une extension finale d'une structure isomorphe à $\mathfrak{M}$; or $\mathfrak{M}(\mathscr{H})$ ne satisfait pas F, et d'après le lemme 4.6, puisque F est Σ, $\mathfrak{M}$ ne satisfait pas F, et donc :

$$\mathfrak{M} \models F \Longrightarrow \exists v_1 \mathfrak{Dem}_0[\underline{\#F}, v_1].$$

⊡

REMARQUE : Cette preuve utilise le théorème de complétude, (nous parlons ici du vrai théorème de complétude, et non de celui qui a été démontré dans $\mathscr{P}$) pour lequel la notion d'ensemble infini et même l'axiome du choix sont nécessaires. Les démonstrations syntaxiques de ce lemme (il en existe) présentent l'avantage de ne faire appel qu'à des notions finies (nombres entiers, suites finies, etc.).

4.9 **Preuve du lemme 2 :**

☹ Considérons la fonction g de $\mathbb{N}$ dans $\mathbb{N}$ définie par :

• si n est le numéro de Gödel d'une formule $F[v_0]$ à une variable libre, alors $g(n)$ est le numéro de Gödel de la formule $F[\underline{n}]$;

• sinon, $g(n) = 0$.

Cette fonction est manifestement récursive primitive, et soit $G[v_0,v_1]$ une formule qui la représente. Pour tout entier n, on a donc :

(1) $\mathscr{P}_0 \vdash \forall v_0(G[v_0,\underline{n}] \Longleftrightarrow v_0 \simeq \underline{g(n)})$.

On définit la formule $\varepsilon[v_0]$ par :

$$\varepsilon[v_0] = \exists v_1 \exists v_2(\mathfrak{Dem}[v_2,v_1] \wedge G[v_2,v_0]).$$

Remarquons que si n est le numéro de Gödel d'une formule $F[v_0]$ à une variable libre, alors :

$$\mathbb{N} \models \varepsilon[\underline{n}] \text{ si et seulement si } F[\underline{n}] \text{ est démontrable.}$$

Soient a le numéro de Gödel de la formule $\neg\varepsilon[v_0]$ et $b = g(a)$, le numéro de Gödel de $\neg\varepsilon[\underline{a}]$. De la définition de ε et de (1), on déduit :

(2) $\mathscr{P}_0 \vdash \varepsilon[\underline{a}] \Longleftrightarrow \exists v_1 \mathfrak{Dem}[\underline{b},v_1]$.

On voit d'abord que T ne démontre pas $\neg\varepsilon[\underline{a}]$. On suppose le contraire, et on en déduit que T est contradictoire. En effet, il existe un entier c qui est le code d'une démonstration de $\neg\varepsilon[\underline{a}]$ dans T, et donc :

$$\mathscr{P}_0 \vdash \mathfrak{Dem}[\underline{b},\underline{c}],$$

ce qui, avec (2), prouve que $\mathscr{P}_0 \vdash \varepsilon[\underline{a}]$. Comme T contient $\mathscr{P}_0$, $T \vdash \varepsilon[\underline{a}]$ et T est donc contradictoire.

Ensuite, on montre que $T \vdash \text{Coh}(T) \Longrightarrow \neg\varepsilon[\underline{a}]$. En fait, on va faire mieux puisqu'on va montrer que $\mathscr{P}_1 \vdash \varepsilon[\underline{a}] \Longrightarrow \neg\text{Coh}(T)$. Posons $T_1 = \mathscr{P}_1 \cup \varepsilon[\underline{a}]$. De (2), on déduit que :

$$T_1 \vdash \exists v_1 \mathfrak{Dem}[\underline{b},v_1].$$

Mais $\varepsilon[\underline{a}]$ est une formule close Σ. Appelons d le numéro de Gödel de $\varepsilon[\underline{a}]$. Alors $\varepsilon[\underline{a}] \Longrightarrow \exists v_2 \mathfrak{Dem}_0[\underline{d},v_2] \in \mathscr{P}_1$ et :

$$T_1 \vdash \exists v_2 \mathfrak{Dem}_0[\underline{d},v_2].$$

Or, on a supposé que $\vdash \forall v_0 \forall v_1(\mathfrak{Dem}_0[v_0,v_1] \Longrightarrow \mathfrak{Dem}[v_0,v_1])$, et donc :

$$T_1 \vdash \exists v_1 \mathfrak{Dem}[\underline{b},v_1] \wedge \exists v_2 \mathfrak{Dem}[\underline{d},v_2],$$

ce qui, en se reportant à la définition de Coh(T), montre bien que :

$$T_1 \vdash \neg \text{Coh}(T),$$

et, grâce au lemme de déduction : $\mathscr{P}_1 \vdash \varepsilon[\underline{a}] \Longrightarrow \neg\text{Coh}(T)$.

☺

REMARQUE 1 : En supposant que la formule $\mathfrak{Dem}$ vérifie quelques propriétés tout à fait anodines et naturelles (essentiellement que :

$$\mathscr{P} \vdash (\exists v_0 \mathfrak{Dem}[\underline{\# F}, v_0] \wedge \exists v_1 \mathfrak{Dem}[\underline{\# (F \Longrightarrow G)}, v_1]) \Longrightarrow \exists v_2 \mathfrak{Dem}[\underline{\# G}, v_2]),$$

on peut voir que la formule Coh(T) est équivalente à $\neg\exists v_0 \mathfrak{Dem}[\#(\underline{0} \simeq \underline{1}), v_0]$.

REMARQUE 2 : La formule $\varepsilon[\underline{a}]$ affirme que sa négation est démontrable. Elle est évidemment fausse dans $\mathbb{N}$.

REMARQUE 3 : Le théorème de Gödel affirme qu'une théorie récursive et cohérente ne peut démontrer sa propre cohérence ; en revanche elle peut très bien démontrer sa propre incohérence, comme c'est le cas pour la théorie $\mathscr{P} \cup \{ \neg\text{Coh}(\mathscr{P}) \}$ par exemple. Toutefois, ce n'est pas le cas pour la théorie $\mathscr{P}$ elle-même : il y a un modèle de $\mathscr{P} \cup \text{Coh}(\mathscr{P})$ (à savoir $\mathbb{N}$) ; ceci se généralise à toute théorie récursive dont $\mathbb{N}$ est un modèle.

EXERCICES

1. Soient X un ensemble non vide et f une fonction de $X \times X$ dans X. On considère la $\mathscr{L}_0$-structure $\mathfrak{M}$ dont l'ensemble de base est $M = \mathbb{N} \cup (X \times \mathbb{Z})$ et où les symboles $\underline{S}$, $\underline{+}$ et $\underline{\times}$ sont interprétés par les fonctions S, + et × définies par les conditions suivantes :

- $\mathfrak{M}$ est une extension de $\mathbb{N}$;
- si $a = (x,n) \in M - \mathbb{N}$, alors $S(a) = (x,n + 1)$;
- si $a = (x,n) \in M - \mathbb{N}$ et $m \in \mathbb{N}$, alors $a + m = m + a = (x,n + m)$;
- si $a = (x,n)$ et $b = (y,m)$ sont des éléments de $M - \mathbb{N}$, alors $(x,n) + (y,m) = (x,n + m)$;
- si $a = (x,n) \in M - \mathbb{N}$ et $m \in \mathbb{N}$, alors $(x,n) \times m = (x,n \times m)$ si $m \neq \mathbf{0}$, et $(x,n) \times \mathbf{0} = \mathbf{0}$;
- si $a = (x,n) \in M - \mathbb{N}$ et $m \in \mathbb{N}$, alors $m \times (x,n) = (x,m \times n)$;
- si $a = (x,n)$ et $b = (y,m)$ sont des éléments de $M - \mathbb{N}$, alors $(x,n) \times (y,m) = (f(x,y),n \times m)$.

a) Montrer que $\mathfrak{M}$ est un modèle de $\mathscr{P}_0$.

b) Montrer qu'aucune des formules suivantes n'est conséquence de $\mathscr{P}_0$:

i) $\forall v_0 \forall v_1\ v_0 \underline{+} v_1 \simeq v_1 \underline{+} v_0$;

ii) $\forall v_0 \forall v_1 \forall v_2\ v_0 \underline{\times} (v_1 \underline{\times} v_2) \simeq (v_0 \underline{\times} v_1) \underline{\times} v_2$;

iii) $\forall v_0 \forall v_1 ((v_0 \leqslant v_1 \wedge v_1 \leqslant v_0) \Longrightarrow v_0 \simeq v_1)$;

iv) $\forall v_0\ \underline{\mathbf{0}} \underline{\times} v_0 \simeq \underline{\mathbf{0}}$.

c) Construire un modèle de $\mathscr{P}_0$ dans lequel l'addition n'est pas associative.

2. Soit $\mathfrak{M}$ un modèle de $\mathscr{P}$ et on suppose que $\mathbb{N}$ est une sous-structure propre de $\mathfrak{M}$. On définit sur M, l'ensemble sous-jacent à $\mathfrak{M}$, la relation $\approx$ suivante : $x \approx y$ si et seulement si il existe deux éléments n et m de $\mathbb{N}$ tels que :

$$\mathfrak{M} \models x \underline{+} \underline{n} \simeq y \underline{+} \underline{m} .$$

a) Montrer que la relation $\approx$ est une relation d'équivalence.

b) Soient a, a', b et b' des éléments de M, tels que $a \approx a'$ et $b \approx b'$. Montrer que $a + b \approx a' + b'$.

c) On appelle E l'ensemble des classes de M relativement à la relation $\approx$. On définit sur E la relation R par : si x et y sont dans E, alors xRy si et seulement si il existe $a \in x$ et $b \in y$ tels que $\mathfrak{M} \models a \leqslant b$.

Montrer que la relation R est une relation d'ordre total. Montrer que E, muni de cet ordre, a un plus petit élément mais pas de plus grand élément. Montrer que R est un ordre dense sur E.

3. Démontrer le théorème chinois (théorème 2.4).

4. Montrer la réciproque du théorème de représentation (théorème 2.2) : si une fonction de $\mathbb{N}^p$ dans $\mathbb{N}$ est représentable, alors elle est récursive.

5. Soit T une théorie dans un langage fini, et on suppose que T est récursivement énumérable, c'est-à-dire que l'ensemble :

$$\{ \# F \, ; F \in T \}$$

est récursivement énumérable. Montrer qu'il existe une théorie T' récursive et équivalente à T (c'est-à-dire telle que, pour toute formule G, G est démontrée par T si et seulement si G est démontrée par T').

6. Montrer que si le « grand théorème de Fermat » :

$$(\forall x > 0)(\forall y > 0)(\forall z > 0)(\forall t > 2)(x^t + y^t \neq z^t)$$

n'est pas réfutable dans $\mathscr{P}_0$, alors il est vrai dans $\mathbb{N}$.
(Ce « grand théorème de Fermat » n'est pas un théorème, puisqu'on ne sait pas le démontrer, ni le réfuter d'ailleurs.)

7. Dans cet exercice, $\mathfrak{Dem}[v_0,v_1]$ est une formule qui représente l'ensemble :

Dem = { (a,b) ; b est le numéro de Gödel d'une démonstration dans $\mathscr{P}$ de la formule dont a est le numéro de Gödel }.

Dire quelles sont, parmi les assertions suivantes, celles qui sont vraies pour toutes les formules closes F :

a) $\mathbb{N} \models \exists v_1 \mathfrak{Dem}[\underline{\# F}, v_1] \Longrightarrow F$;

b) $\mathscr{P} \vdash \exists v_1 \mathfrak{Dem}[\underline{\# F}, v_1] \Longrightarrow F$;

c) $\mathbb{N} \models F \Longrightarrow \exists v_1 \mathfrak{Dem}[\underline{\# F}, v_1]$;

d) $\mathscr{P} \vdash F \Longrightarrow \exists v_1 \mathfrak{Dem}[\underline{\# F}, v_1]$.

8. Montrer qu'il existe une formule $F[v_0]$ de $\mathscr{L}_0$ telle que $\mathbb{N} \models \neg\exists v_0 F[v_0]$ et $\mathscr{P}$ ne démontre pas $\neg\exists v_0 F[v_0]$. En déduire que, pour toute formule $G[v_0,v_1,\ldots,v_n]$, il existe une formule $H[v_0,v_1,\ldots,v_n]$ telle que :

$$\forall v_0 \forall v_1 \ldots \forall v_n (G[v_0,v_1,\ldots,v_n] \Longleftrightarrow H[v_0,v_1,\ldots,v_n])$$

soit vraie dans $\mathbb{N}$ mais non démontrable dans $\mathscr{P}$.

9. Montrer que, si F est une formule close et si :

$$\mathscr{P} \vdash \exists v_0 \mathfrak{Dem}[\underline{\# F}, v_0] \Longrightarrow F,$$

alors :

$$\mathscr{P} \vdash F.$$

(Voir exercice 7 ; on pourra appliquer le second théorème d'incomplétude à la théorie $\mathscr{P} \cup \{ \neg F \}$.)

10. Cet exercice utilise la notion d'**extension élémentaire** qui sera introduite au chapitre 8 (théorie des modèles).

Soient $\mathfrak{M}$ un modèle non standard de $\mathscr{P}$, M l'ensemble sous-jacent à $\mathfrak{M}$, et $A \subseteq M$. On dit qu'une fonction f de M^p dans M est **définissable à paramètres dans** A s'il existe une formule $F[v_0,v_1,v_2,\ldots,v_p]$ de $\mathscr{L}_0$ à paramètres dans A telle que, pour tous $a_1,a_2,\ldots,a_p$ appartenant à M, on ait :

$$\mathfrak{M} \models \forall v_0(F[v_0,a_1,a_2,\ldots,a_p] \Longleftrightarrow v_0 \simeq f(a_1,a_2,\ldots,a_p)).$$

a) Soit $\mathfrak{N}$ une sous-structure de $\mathfrak{M}$, dont l'ensemble sous-jacent, noté N, est clos pour les fonctions définissables à paramètres dans N (c'est-à-dire tel que pour $p \in \mathbb{N}$, pour toute fonction f de M^p dans M définissable à paramètres dans N, et pour tous $a_1,a_2,\ldots,a_p$ de N, $f(a_1,a_2,\ldots,a_p) \in N$).

Montrer que $\mathfrak{N}$ est une sous-structure élémentaire de $\mathfrak{M}$ (et donc un modèle de $\mathscr{P}$).
(Indice : montrer par induction sur la hauteur de la formule G à paramètres dans $\mathfrak{N}$ que G est vraie dans $\mathfrak{N}$ si et seulement si elle est vraie dans $\mathfrak{M}$.)

b) On dit maintenant qu'un sous-ensemble X de M^p est **définissable à paramètres dans** A s'il existe une formule $G[v_1,v_2,\ldots,v_p]$ à paramètres dans A telle que, pour tous $a_1,a_2,\ldots,a_p$ de M,

$$(a_1,a_2,\ldots,a_p) \in X \text{ si et seulement si } \mathfrak{M} \models G[a_1,a_2,\ldots,a_p].$$

Montrer que l'ensemble des sous-ensembles de M définissables à paramètres dans A forment une sous-algèbre de Boole de l'algèbre de tous les sous-ensembles de M.

Montrer que, si f et g sont des fonctions de M dans M définissables à paramètres dans A, alors l'ensemble $\{ a \in M ; f(a) = g(a) \}$ est définissable à paramètres dans A.

c) Soient f et g deux applications de M dans M. On définit les applications Sf, $f + g$ et $f \times g$ de M dans M par :

$$Sf(x) = f(x) + 1 \quad ; \quad (f + g)(x) = f(x) + g(x) \quad ; \quad (f \times g)(x) = f(x) \times g(x).$$

Montrer que l'ensemble des fonctions définissables à paramètres dans A est clos pour ces opérations.

d) Soient $\mathscr{B}$ l'algèbre de Boole des sous-ensembles de M définissables à paramètres dans M, $\mathscr{U}$ un ultrafiltre de cette algèbre et $\mathscr{F}$ l'ensemble des fonctions de M dans M définissables à paramètres dans M.

Montrer que la relation $\approx$ sur $\mathscr{F}$, définie par :

$$f \approx g \text{ si et seulement si } \{ a \in M ; f(a) = g(a) \} \in \mathscr{U},$$

est une relation d'équivalence et que, si $f \approx f'$ et $g \approx g'$, alors :

$$Sf \approx Sf' \quad f + g \approx f' + g' \quad \text{et} \quad f \times g \approx f' \times g'.$$

Si $f \in \mathscr{F}$, on note $f/\mathscr{U}$ la classe de f relativement à $\approx$ et $\mathscr{F}/\mathscr{U}$ l'ensemble des classes relativement à la relation $\approx$. On voit donc que l'on peut définir sur $\mathscr{F}/\mathscr{U}$ les opérations S,+,×. L'élément **0** de $\mathscr{F}/\mathscr{U}$ sera par définition la classe de la fonction

constante égale à $\mathbf{0}$. Cela permet donc de considérer $\mathscr{F}/\mathscr{U}$ comme une $\mathscr{L}_0$-structure.

e) Soit, pour chaque $a \in M$, l'élément $\bar{a}$ de $\mathscr{F}/\mathscr{U}$ égal à la classe relativement à $\approx$ de la fonction constante égale à a.

Montrer que l'application de $\mathfrak{M}$ dans $\mathscr{F}/\mathscr{U}$ qui à $a \in M$ fait correspondre $\bar{a}$ est un homomorphisme de $\mathscr{L}_0$-structures.

f) Montrer que, pour tout $p \in \mathbb{N}$, pour toute formule $F[v_1,v_2,\ldots,v_p]$ de $\mathscr{L}_0$ et pour tous $f_1,f_2,\ldots,f_p$ de $\mathscr{F}$ on a :
$\mathscr{F}/\mathscr{U} \models F[f_1/\mathscr{U}, f_2/\mathscr{U},\ldots,f_p/\mathscr{U}]$ si et seulement si $\{a \in M ; \mathfrak{M} \models F[f_1(a),f_2(a),\ldots,f_p(a)]\} \in \mathscr{U}$.

En déduire que l'application de $\mathfrak{M}$ dans $\mathscr{F}/\mathscr{U}$ qui à $a \in M$ fait correspondre $\bar{a}$ est élémentaire (voir chapitre 8).

g) On suppose que $\mathbb{N}$ est une sous-structure élémentaire de $\mathfrak{M}$. Montrer que, si f est une fonction de M dans M, définissable à paramètres dans $\mathfrak{M}$, et si $a \in M$, alors il existe $b \in M$ tel que :

$$\mathfrak{M} \models \forall v_0(v_0 < a \Longrightarrow f(v_0) < b).$$

h) Soit $\mathfrak{M}$ une extension élémentaire propre de $\mathbb{N}$. Montrer qu'il existe une extension élémentaire propre $\mathfrak{N}$ de $\mathfrak{M}$ de base N telle que : pour tout $a \in N$, il existe $b \in M$ tel que :

$$\mathfrak{N} \models a < b .$$

11. Soient $\mathscr{L}$ un langage fini, $\mathfrak{M}$ une $\mathscr{L}$-structure et M son ensemble sous-jacent. On dit que $\mathfrak{M}$ est **fortement indécidable** si toute théorie dans $\mathscr{L}$ dont $\mathfrak{M}$ est modèle est indécidable.

a) Montrer que $\mathbb{N}$ est fortement indécidable.

b) On fixe cinq formules de $\mathscr{L}$: $G_0[v_0]$, $G_1[v_0]$, $G_2[v_0,v_1]$, $G_3[v_0,v_1,v_2]$, $G_4[v_0,v_1,v_2]$, et on considère la théorie T_0 dont les axiomes sont les formules suivantes :

(1) $\forall v_0(G_1[v_0] \Longrightarrow G_0[v_0])$;
(2) $\forall v_0 \forall v_1(G_2[v_0,v_1] \Longrightarrow (G_0[v_0] \wedge G_0[v_1]))$;
(3) $\forall v_0 \forall v_1 \forall v_2(G_3[v_0,v_1,v_2] \Longrightarrow (G_0[v_0] \wedge G_0[v_1] \wedge G_0[v_2]))$;
(4) $\forall v_0 \forall v_1 \forall v_2(G_4[v_0,v_1,v_2] \Longrightarrow (G_0[v_0] \wedge G_0[v_1] \wedge G_0[v_2]))$;
(5) $\exists! v_0 G_1[v_0]$;
(6) $\forall v_1(G_0[v_1] \Longrightarrow \exists! v_0 G_2[v_0,v_1])$;
(7) $\forall v_1 \forall v_2((G_0[v_1] \wedge G_0[v_2]) \Longrightarrow \exists! v_0 G_3[v_0,v_1,v_2])$;
(8) $\forall v_1 \forall v_2((G_0[v_1] \wedge G_0[v_2]) \Longrightarrow \exists! v_0 G_4[v_0,v_1,v_2])$.

Si $\mathfrak{M}$ est un modèle de T_0, on définit la $\mathscr{L}_0$-structure $\mathfrak{N}$ de la façon suivante : l'ensemble de base de $\mathfrak{N}$ est $N = \{a \in \mathfrak{M} ; \mathfrak{M} \models G_0[a]\}$; la constante $\underline{0}$ est interprétée par l'unique élément a de $\mathfrak{M}$ satisfaisant $G_1[a]$, le symbole $\underline{S}$ est interprété par la fonction qui à $a \in N$ fait correspondre l'unique élément b tel que $\mathfrak{M} \models G_2[b,a]$, le symbole $\underline{+}$ par la fonction qui à deux éléments a et b de N fait correspondre l'unique élément c tel que

$\mathfrak{M} \models G_3[c,a,b]$, le symbole $\underline{\times}$ par la fonction qui à deux éléments a et b de N fait correspondre l'unique élément c tel que $\mathfrak{M} \models G_4[c,a,b]$. On dira que **$\mathfrak{N}$ est définissable dans $\mathfrak{M}$** (attention à ne pas faire de confusion avec la notion de sous-ensemble définissable).

Montrer que, pour toute formule $F[v_1,v_2,\dots,v_p]$ de $\mathcal{L}_0$, il existe une formule $F^*[v_1,v_2,\dots,v_p]$ de $\mathcal{L}$ telle que, si $\mathfrak{M}$ est un modèle de T_0 et $\mathfrak{N}$ est la $\mathcal{L}_0$-structure définie dans $\mathfrak{M}$, et si $a_1,a_2,\dots,a_p$ sont des éléments de N, alors :

$$\mathfrak{N} \models F[a_1,a_2,\dots,a_p] \text{ si et seulement si } \mathfrak{M} \models F^*[a_1,a_2,\dots,a_p].$$

Montrer que F^* peut être trouvée effectivement à partir de la formule F, c'est-à-dire : il existe une fonction α récursive primitive telle que, si $n = \# F$, alors $\alpha(n) = \# F^*$.

c) Soit T une théorie de $\mathcal{L}$ contenant T_0. On pose :

$$T^- = \{ F ; F \text{ est une formule close de } \mathcal{L}_0 \text{ et } T \vdash F^* \}.$$

Montrer que si G est une formule close de $\mathcal{L}_0$, les trois conditions suivantes sont équivalentes : 1) $G \in T^-$; 2) $T^- \vdash G$; 3) $T \vdash G^*$.

d) Montrer que si $\mathbb{N}$ est définissable dans $\mathfrak{M}$, alors $\mathfrak{M}$ est fortement indécidable.

e) Montrer que la structure $\mathbb{Z}$ dans le langage des anneaux $\mathcal{L} = \{\underline{0},\underline{+},\underline{\times}\}$ est fortement indécidable (utiliser le théorème de Lagrange : tout entier positif est la somme de quatre carrés). Montrer que les théories suivantes sont indécidables : la théorie des anneaux, la théorie des anneaux commutatifs, la théorie des anneaux intègres.

f) On suppose que $\mathcal{L}$ est le langage ne contenant qu'un seul symbole de prédicat binaire R. On considère la $\mathcal{L}$-structure $\mathfrak{M}$ dont l'ensemble sous-jacent est $M = \mathbb{N} \cup (\mathbb{N} \times \mathbb{N})$ et où $R^{\mathfrak{M}}$ est égal à :

$\{(a,(a,b)) ; a \in \mathbb{N}, b \in \mathbb{N}\} \cup \{((a,b),b) ; a \in \mathbb{N}, b \in \mathbb{N}\} \cup \{((a,b),(a+b,a\cdot b)) ; a \in \mathbb{N}, b \in \mathbb{N}\}$.

Montrer que $\mathbb{N}$ est interprétable dans $\mathfrak{M}$. Montrer que l'ensemble des formules universellement valides du langage $\mathcal{L}$ n'est pas récursif.

g) Cette fois, $\mathcal{L}$ est le langage contenant un symbole de prédicat binaire D et un symbole de fonction binaire $\underline{+}$. Soit $\mathfrak{M}$ la $\mathcal{L}$-structure dont l'ensemble sous-jacent est $\mathbb{N}$, où $\underline{+}$ est interprété par l'addition et D par la relation « divise » (Dxy est vrai si et seulement si x divise y).

Montrer que l'élément 1 et la relation $x = y\cdot(y+1)$ sont définissables dans $\mathfrak{M}$. Montrer que $\mathfrak{M}$ est fortement indécidable.

12. Soient f une fonction récursive totale de $\mathbb{N}$ dans $\mathbb{N}$ et $F[v_0,v_1]$ une formule Σ la représentant (voir théorème 4.6). On a alors :

$$\mathbb{N} \models \forall v_1 \exists v_0\, F[v_0,v_1].$$

On dit que f est **prouvablement totale** s'il existe une formule Σ la représentant et telle que :

$$\mathcal{P} \vdash \forall v_1 \exists v_0\, F[v_0,v_1].$$

Le but de cet exercice est de montrer qu'il existe des fonctions récursives totales qui ne sont pas prouvablement totales.

a) Soit $F[v_0,v_1,...,v_k]$ une formule Σ. Montrer que l'ensemble :

$$\{ (n_0,n_1,...,n_k) \; ; \; \mathbb{N} \models F[n_0,n_1,...,n_k] \}$$

est récursivement énumérable.

b) Soit f une fonction totale de $\mathbb{N}$ dans $\mathbb{N}$; montrer que les deux conditions suivantes sont équivalentes :

i) f est récursive ;

ii) il existe une formule Σ qui représente f.

c) Montrer qu'il existe une fonction partielle récursive h à 2 variables telle que, pour tout entier n :

• si a est le numéro de Gödel d'une formule Σ, disons $F[v_0,v_1]$, et s'il existe un entier m tel que $\mathscr{P} \vdash F[\underline{m},\underline{n}]$, alors :

$$\mathscr{P} \vdash F[\underline{h(a,n)},\underline{n}] \; ;$$

• si a est le numéro de Gödel de la formule $F[v_0,v_1]$, et s'il n'existe pas d'entier m tel que $\mathscr{P} \vdash F[\underline{m},\underline{n}]$, alors $h(a,n)$ n'est pas définie ;

• sinon, $h(a,n) = 0$.

d) On définit maintenant une fonction g de $\mathbb{N}^3$ dans $\mathbb{N}$ de la façon suivante : pour tout entier n :

• si a est le numéro de Gödel d'une formule sigma $F[v_0,v_1]$ et si b est le numéro de Gödel d'une démonstration dans $\mathscr{P}$ de la formule :

$$\forall v_1 \exists v_0 F[v_0,v_1],$$

alors $g(a,b,n) = h(a,n)$;

• sinon, $g(a,b,n) = 0$.

Montrer que g est une fonction totale récursive.

e) Montrer qu'il existe des fonctions récursives totales qui ne sont pas prouvablement totales.

13. Cet exercice doit être fait après la lecture du chapitre 7 sur la théorie des ensembles. En particulier on doit savoir ce qu'est le cardinal $2^{\aleph_0}$.

a) Montrer que, si T est une théorie cohérente obtenue à partir de $\mathscr{P}$ en y ajoutant un nombre fini de formules, alors T n'est pas complète.

b) Construire, pour chaque entier n et chaque $s = (s(0),s(1),...,s(n-1)) \in \{0,1\}^n$, une formule close F_s, de sorte que, pour tout s :

i) $F_{(s(0),s(1),...,s(n-1),1)} = \neg F_{(s(0),s(1),...,s(n-1),0)}$;

ii) $\mathscr{P} \cup \{ F_{\emptyset}, F_{(s(0))}, F_{(s(0),s(1))}, ..., F_{(s(0),s(1),...,s(n-1))} \}$ est une théorie cohérente.

c) Montrer qu'il existe $2^{\aleph_0}$ théories contenant $\mathscr{P}$ et deux à deux non équivalentes.

14. Pour cet exercice aussi, il faut avoir des notions de théorie des ensembles. Il faut également connaître un peu de théorie des modèles (extensions élémentaires et méthode des diagrammes).

Soient $\mathfrak{M}$ une extension élémentaire de $\mathbb{N}$ et X un sous-ensemble de $\mathbb{N}$. Rappelons (5.12, chapitre 3) que X est définissable dans $\mathfrak{M}$ s'il existe une formule F de $\mathscr{L}_0$ à une variable libre et à paramètres dans $\mathfrak{M}$ telle que, pour tout $n \in \mathbb{N}$,

$$n \in X \quad \text{si et seulement si} \quad \mathfrak{M} \models F[n].$$

a) Montrer que, si $\mathfrak{M}$ est dénombrable, l'ensemble des sous-ensembles de $\mathbb{N}$ définissables dans $\mathfrak{M}$ est dénombrable.

b) Montrer que, pour tout sous-ensemble X de $\mathbb{N}$, il existe une extension élémentaire dénombrable $\mathfrak{M}$ de $\mathbb{N}$ dans laquelle X est définissable.

c) Montrer qu'il existe $2^{\aleph_0}$ extensions élémentaires dénombrables de $\mathbb{N}$ deux à deux non isomorphes.

15. a) Qu'y a-t-il de paradoxal dans l'affirmation d'Epiménides (voir l'introduction) ?

b) Dans un village des Carpates, vit un barbier qui rase tous les hommes qui ne se rasent pas eux-mêmes et seulement ceux-là. Que pouvez-vous dire de ce barbier ?

Chapitre 7

Théorie des ensembles

Le but de la théorie des ensembles, créée au début du siècle par G. Cantor, est de permettre de construire toutes les mathématiques en utilisant seulement la notion d'appartenance.

On exposera dans ce chapitre les axiomes de Zermelo–Fraenkel (ZF) sous forme d'une théorie du premier ordre, dans un langage ne comportant que deux symboles de prédicat binaire, l'égalité et l'appartenance. A part l'extensionnalité qui a un rôle particulier, les axiomes de ZF affirment l'existence d'ensembles. Certains, comme l'axiome de la paire ou celui de la réunion, ne surprendront personne, mais d'autres peuvent paraître moins naturels. Il faut comprendre qu'ils sont le fruit d'un compromis : ils doivent, d'une part, permettre de construire tous les ensembles dont la pratique mathématique a besoin, et, d'autre part, il ne doivent pas être contradictoires comme c'est le cas (et cela s'est effectivement produit historiquement) si les axiomes sont introduits sans discernement.

L'axiome du choix, lui, est carrément incompréhensible au premier abord. Il paraît en effet tellement évident qu'il semble même inutile de le mentionner. A ce propos, il faut bien comprendre que l'on raisonne axiomatiquement, et que, comme il ne se déduit pas des autres axiomes, il faut bien le rajouter. Par ailleurs, il a des conséquences tout-à-fait surprenantes et même paradoxales, comme le théorème de Banach-Tarski qui permet de découper une sphère S *en deux parties homéomorphes à* S. *De toute façon, quelle que soit l'estime dans laquelle on tient cet axiome, il faut savoir que les mathématiciens l'emploient couramment.*

On fera, au début de ce chapitre, le travail consistant à traduire les notions mathématiques usuelles dans le langage de la théorie des ensembles : on verra rapidement comment définir les relations, les applications ; on montrera comment définir des éléments pouvant prétendre à jouer le rôle d'entiers, et le lecteur pourra se convaincre de la possibilité de construire $\mathbb{R}$, $\mathbb{C}$, *et toute structure dont il pourrait avoir besoin.*

La théorie des ensembles fournit un certain nombre d'outils que l'on utilise en mathématiques. Il y a, en premier lieu, le lemme de Zorn. On a vu, au chapitre 5, comment les entiers permettent d'énumérer des ensembles apparemment plus compliqués, comme $\mathbb{N} \times \mathbb{N}$, *l'ensemble des suites finies d'entiers, ou même l'ensemble des fonctions récursives. Les ordinaux, qui sont une sorte de généralisation des entiers, permettent, du moins si on admet l'axiome du choix, d'énumérer n'importe quel ensemble. La cardinalité est aussi une notion importante : elle permet de compter le nombre d'éléments d'un ensemble. Deux ensembles ont le même nombre d'éléments (on dit « ont même cardinalité ») s'il existe une bijection de l'un sur l'autre. Ceci oblige à distinguer plusieurs « tailles d'infinité » : par exemple,* $\mathbb{R}$ *et* $\mathbb{N}$ *ne peuvent pas être mis en*

bijection. Cette notion nous réserve aussi des surprises : un ensemble peut avoir le même nombre d'éléments qu'une de ses parties propres.

Enfin, quittant les mathématiques classiques, on fera aussi une brève étude des modèles de la théorie des ensembles. Là, l'outil essentiel est la hiérarchie des V_α, *qui justifiera l'introduction d'un nouvel axiome, l'axiome de fondation. Il permet notamment de répondre négativement à une question naturelle (existe-t-il un ensemble a s'appartenant à lui-même ?) à laquelle les axiomes de ZF seuls ne peuvent apporter de réponse. Cela aboutira à quelques résultats de consistance relative, par exemple : si ZF est une théorie consistante, alors ZF plus l'axiome de fondation est aussi une théorie consistante.*

1. LES THEORIES Z ET ZF

Les axiomes

1.1 Nous allons présenter la théorie des ensembles comme une théorie du premier ordre. Le langage $\mathscr{L}$ de cette théorie ne comporte, en plus de l'habituel symbole de l'égalité $\simeq$, qu'un symbole de prédicat binaire $\in$, appelé symbole de l'**appartenance**. En fait, on donnera les axiomes de plusieurs théories des ensembles, plus ou moins fortes. Dans tout ce chapitre et sauf mention du contraire, $\mathfrak{U}$ désignera un modèle de la théorie ZF (voir plus loin) (avant 2.7, point où sera introduit le dernier axiome de ZF, $\mathfrak{U}$ désignera un modèle de ceux des axiomes de ZF qui auront été jusque là introduits). L'ensemble de base de $\mathfrak{U}$ sera noté $\mathscr{U}$ et sera appelé **univers**. Lorsqu'on dira qu'une formule est vraie, on sous-entendra toujours : « dans $\mathfrak{U}$ ».

On se heurte à une difficulté que l'on a déjà rencontrée plusieurs fois : les mots « ensemble », « appartient » etc. dans leur sens intuitif sont d'un usage constant dans les textes mathématiques. Or, le but de ce chapitre est de formaliser ces notions, et on voit que l'on aura besoin de deux niveaux de langage et de raisonnement : d'une part le langage formalisé $\mathscr{L}$ utilisé pour faire des démonstrations qui, théoriquement du moins, pourraient être formalisées dans le sens du chapitre 4 ; et d'autre part le métalangage qui nous permettra de parler de $\mathscr{L}$, des interprétations des symboles de $\mathscr{L}$ dans $\mathfrak{U}$, des théories exprimées dans $\mathscr{L}$ ou de leurs modèles. Par exemple, la formule $\exists v_0 \forall v_1 \neg v_1 \in v_0$

fait partie du langage formalisé ; par contre, lorsqu'on parle de la longueur de cette formule ou du fait qu'elle est démontrable dans ZF, il s'agit du métalangage. En fait, ces deux langages s'appliquent à deux univers différents : le premier à $\mathfrak{U}$, le second à l'univers familier aux mathématiciens, le méta-univers, qui comporte, entre autres, la notion d'entier, de suite finie, et même d'ensemble. Il est essentiel d'éviter toute confusion.

Pour cela, un certain nombre de mots et de symboles seront réservés à un usage purement formel : ainsi, tout d'abord, le symbole $\in$ qui désignera toujours la relation entre points de $\mathcal{U}$ (on se permet tout de même la confusion entre $\in$ et ce que nous aurions, au chapitre 3, noté $\overline{\in}^{\mathfrak{A}}$). Un ensemble sera toujours un point de $\mathcal{U}$ (en conséquence, on s'interdira de parler de l'ensemble $\mathcal{U}$). Lorsqu'on dira que x est un élément de y, cela voudra toujours dire que x et y sont des ensembles (i.e. des points de $\mathcal{U}$) et que

$$\mathfrak{U} \models x \in y.$$

Mais cela ne s'arrête pas là. On veut aussi, en se servant de la théorie des ensembles, formaliser toutes les mathématiques. On sera amené à définir la notion de relation, d'application, et même d'entier naturel. Aussitôt que les définitions seront données, les mots correspondants seront réservés à l'usage formel. Il arrivera que l'on doive utiliser des objets du méta-univers, par exemple les entiers pour faire une récurrence sur la longueur d'une formule de $\mathcal{L}$: dans ce cas, on emploiera l'adjectif « intuitif » ou le préfixe « méta » (entier intuitif, méta-relation, etc.).

A l'exception de ceux de la dernière section, tous les théorème énoncés dans ce chapitre sont des théorèmes de ZF, ou, lorsque c'est précisé, de ZFC (ZF plus l'axiome du choix). En ce sens, il s'agit d'un exposé axiomatique de la théorie des ensembles. Mais, bien évidemment, nous adopterons l'attitude habituelle en mathématiques : notre souci sera de convaincre le lecteur de la véracité des théorèmes plutôt que d'en donner un démonstration formelle. Pour ne pas ajouter de complications aux problèmes de langage, on se dispensera de distinguer, comme on l'a déjà signalé, le symbole $\in$ et son interprétation dans $\mathfrak{U}$ ou dans les autres modèles que l'on aura à manipuler.

On écrira $x \notin y$ comme abréviation de la formule $\neg x \in y$. On emploiera aussi librement les abréviations suivantes :

$\forall x \in y\ F$ pour $\forall x(x \in y \Rightarrow F)$ et $\exists x \in y\ F$ pour $\exists x(x \in y \wedge F)$

(x et y étant des symboles de variables et F une formule).

1.2 Voici la liste des axiomes que l'on va énoncer et commenter : l'axiome d'extensionnalité, l'axiome de la paire, l'axiome de la réunion, l'axiome des parties, les axiomes de compréhension, les axiomes de remplacement. L'axiome du choix (AC) et l'axiome de l'infini (Inf) seront présentés un peu plus tard.

Les axiomes d'extensionnalité, de la paire, de la réunion, des parties, de compréhension et de l'infini constituent ce qu'on appelle habituellement la **théorie des**

ensembles de Zermelo, notée Z ; les axiomes d'extensionnalité, de la paire, de la réunion, des parties, de remplacement et de l'infini forment une théorie plus forte, la **théorie de Zermelo-Fraenkel** (notée ZF). A part l'extensionnalité, chacun des axiomes de Z ou de ZF permet la construction d'un ensemble à partir d'autres ; l'axiome d'extensionnalité en garantit l'unicité.

On notera respectivement Z^- et ZF^- les théories obtenues en supprimant l'axiome de l'infini de Z et de ZF. Enfin ZFC est la théorie ZF plus l'axiome du choix.

• **L'axiome d'extensionnalité** exprime que deux ensembles ayant les mêmes éléments sont égaux :

$\forall v_0 \forall v_1 (\forall v_2 (v_2 \in v_0 \Longleftrightarrow v_2 \in v_1) \Longrightarrow v_0 \simeq v_1)$.

Soient a et b deux ensembles. On dit que a est un **sous-ensemble** de b, ou bien que a **est inclus dans** b, ou encore que a **est une partie** de b, si tout élément de a est un élément de b. Autrement dit, si, dans $\mathfrak{U}$, a et b satisfont :

$$\forall v_0 (v_0 \in a \Longrightarrow v_0 \in b).$$

Cette formule sera abrégée par $a \subseteq b$; $a \subsetneq b$ est la formule $a \subseteq b \wedge \neg a \simeq b$.

L'axiome d'extensionnalité sera utilisé lorsqu'on voudra montrer que deux ensembles a et b sont égaux : on montrera que $a \subseteq b$ et que $b \subseteq a$.

• **Axiome de la paire** :

$\forall v_0 \forall v_1 \exists v_2 \forall v_3 (v_3 \in v_2 \Longleftrightarrow (v_3 \simeq v_0 \vee v_3 \simeq v_1))$.

Etant donnés deux ensembles a et b, il existe un ensemble dont les seuls éléments sont a et b. D'après l'axiome d'extensionnalité, il n'y en a qu'un seul ; on le note $\{a,b\}$, et on l'appelle **la paire** a,b.

Il est possible que a soit égal à b. Dans ce cas, on obtient un ensemble qui n'a qu'un seul élément ; on le note $\{a\}$ au lieu de $\{a,a\}$ et on l'appelle **singleton** a.

On remarque que :

$\{a,b\} = \{a',b'\}$ si et seulement si $(a = a'$ et $b = b')$ ou $(a = b'$ et $b = a')$,

et que : $\{a\} = \{a'\}$ si et seulement si $a = a'$.

• **Axiome de la réunion** :

$\forall v_0 \exists v_1 \forall v_2 (v_2 \in v_1 \Longleftrightarrow \exists v_3 (v_3 \in v_0 \wedge v_2 \in v_3))$.

Etant donné un ensemble a, cet axiome affirme l'existence d'un ensemble dont les éléments sont les éléments des éléments de a, autrement dit qui est la réunion de tous les ensembles qui appartiennent à a. Toujours par extensionnalité, cet ensemble est unique ; on le note $\bigcup_{x \in a} x$, ou plus simplement $\bigcup a$.

1.3 Voyons, avant d'aller plus loin, quelques conséquences de ces trois axiomes. Soient a et b deux ensembles. Grâce à l'axiome de la paire, on peut former l'ensemble

$c = \{a,b\}$, puis, avec avec l'axiome de la réunion, $\bigcup c$. Cet ensemble est appelé la **réunion de** a et b et est noté $a \cup b$. Il vérifie :

$$\forall v_0(v_0 \in a \cup b \Longleftrightarrow (v_0 \in a \lor v_0 \in b)).$$

Considérons maintenant trois ensembles a, b et c. On peut former les ensembles $\{a,b\}$ et $\{c\}$, puis la réunion de ces deux derniers ensembles $\{a,b\} \cup \{c\}$, que l'on note $\{a,b,c\}$. On voit alors que :

$$\forall v_0(v_0 \in \{a,b,c\} \Longleftrightarrow (v_0 \simeq a \lor v_0 \simeq b \lor v_0 \simeq c))$$

est vraie. On peut itérer le processus et voir que, si n est un entier strictement positif (dans le sens intuitif) et si $a_1, a_2, \ldots, a_n$ sont des ensembles, alors il existe un ensemble, noté $\{a_1,a_2,\ldots,a_n\}$, vérifiant :

$$\forall v_0(v_0 \in \{a_1,a_2,\ldots,a_n\} \Longleftrightarrow (v_0 \simeq a_1 \lor v_0 \simeq a_2 \lor \ldots \lor v_0 \simeq a_n)).$$

On peut aussi former $\bigcup \{a_1,a_2,\ldots,a_n\}$, que l'on note $a_1 \cup a_2 \cup \ldots \cup a_n$ et on a :

$$\forall v_0(v_0 \in a_1 \cup a_2 \cup \ldots \cup a_n \Longleftrightarrow (v_0 \in a_1 \lor v_0 \in a_2 \lor \ldots \lor v_0 \in a_n)).$$

1.4 • **Axiome des parties** : l'axiome des parties affirme que, étant donné un ensemble a, il existe un ensemble b, unique par extensionnalité, noté $\mathfrak{P}(a)$, dont les éléments sont exactement les parties de a :

$$\forall v_0 \exists v_1 \forall v_2(v_2 \in v_1 \Longleftrightarrow \forall v_3(v_3 \in v_2 \Longrightarrow v_3 \in v_0)).$$

• **Schéma d'axiome de compréhension**. Il s'agit cette fois, non pas d'un axiome mais d'une infinité d'axiomes. Ce sont toutes les formules qui peuvent s'écrire sous la forme :

$$\forall v_1 \forall v_2 \ldots \forall v_{n+1} \exists v_{n+2} \forall v_0(v_0 \in v_{n+2} \Longleftrightarrow (v_0 \in v_{n+1} \land F[v_0,v_1,\ldots,v_n]))$$

où n est un entier et $F[v_0,v_1,\ldots,v_n]$ est une formule de $\mathscr{L}$.

Ce schéma signifie donc que, étant donnés un ensemble a et une formule $H[v_0]$ à une variable libre et avec des paramètres dans $\mathscr{U}$, il y a un ensemble, unique par extensionnalité, dont les éléments sont précisément ceux des éléments de a qui satisfont H. On notera $\{x \in a ; H[x]\}$ cet ensemble.

On peut se demander pourquoi on s'embarrasse de l'ensemble a : il semblerait plus facile et plus naturel de considérer le schéma d'axiome suivant : pour toute formule $H[v_0]$ à une variable libre et à paramètres dans $\mathscr{U}$, il existe un ensemble dont les éléments sont les ensembles vérifiant H :

$$\forall v_1 \forall v_2 \ldots \forall v_n \exists v_{n+1} \forall v_0(v_0 \in v_{n+1} \Longleftrightarrow F[v_0,v_1,\ldots,v_n])$$

(n entier, $F[v_0,v_2,\ldots,v_n]$ formule de $\mathscr{L}$).

En fait, il y a une bonne raison pour ne pas admettre ce schéma : la théorie que l'on obtiendrait est contradictoire. En effet, avec la formule $F = v_0 \notin v_0$, on obtient :

$$\exists v_1 \forall v_0(v_0 \in v_1 \Longleftrightarrow v_0 \notin v_0).$$

Il existerait donc un ensemble a tel que, pour tout ensemble b,

$$b \in a \Longleftrightarrow b \notin b.$$

En particulier, pour $b = a$, on obtient :

$$a \in a \Longleftrightarrow a \notin a,$$

ce qui est manifestement contradictoire.

Le lecteur aura évidemment reconnu l'argument diagonal cher aux logiciens. La contradiction apparente qu'il produit est connue sous le nom de **paradoxe de Russell**. Cet argument peut être employé pour montrer qu'il n'existe pas d'« ensemble de tous les ensembles ». Exactement :

THEOREME : *Si* $\mathfrak{U}$ *est un modèle de* Z^-, *alors*

$$\mathfrak{U} \models \neg\exists v_0 \forall v_1 (v_1 \in v_0).$$

☹ Supposons le contraire : appelons a l'ensemble tel que

$$\forall v_0 \; v_0 \in a,$$

et appliquons le schéma de compréhension avec $v_1 = a$ et $F = v_0 \notin v_0$. On obtient encore un ensemble b tel que

$$\forall v_0 (v_0 \in b \Longleftrightarrow v_0 \notin v_0),$$

ce qui mène encore à une contradiction, lorsque v_0 prend la valeur b.

☺

On a dit que l'on réserverait le mot « ensemble » aux points de $\mathscr{U}$. Pourtant, il est parfois commode de parler de la collection (c'est-à-dire du sous-ensemble au sens intuitif) des points de $\mathscr{U}$ satisfaisant telle ou telle propriété du premier ordre. On utilisera le mot « classe » pour désigner ces collections : si $F[v_0]$ est n'importe quelle formule de $\mathscr{L}$ à une variable libre, avec paramètres dans $\mathscr{U}$, on pourra évoquer la classe des ensembles a satisfaisant $F[a]$. Les classes ne sont donc rien d'autre que les « sous-ensembles intuitifs » définissables avec paramètres dans la structure $\mathfrak{U}$ (voir chapitre 3, 5.12). En fait, on pourrait, au prix d'un alourdissement considérable de l'exposé, éviter l'utilisation de la notion de « classe ». Pour éviter les malentendus, on utilisera les majuscules script ($\mathscr{U}$, $\mathscr{V}$ etc.) pour désigner ces classes. Si $F[v_0]$ est une formule et $\mathscr{A}$ la classe des ensembles a satisfaisant $F[a]$, on dira qu'un ensemble b fait partie de $\mathscr{A}$, ou que $\mathscr{A}$ contient b pour dire que b satisfait F. On fera l'abus de langage consistant à identifier un ensemble a avec la classe des ensembles b appartenant à a. A l'exception de l'axiome d'extensionnalité, les axiomes que nous avons énoncés jusqu'à présent (et il en sera de même des axiomes de remplacement) expriment que certaines classes sont des ensembles.

1.5 Voici maintenant quelques conséquences des axiomes de compréhension. Tout d'abord, en prenant pour F la formule $\neg v_0 \simeq v_0$, on obtient :

$$\forall v_1 \exists v_2 \forall v_0 (v_0 \in v_2 \Longleftrightarrow (v_0 \in v_1 \land \neg v_0 \simeq v_0)).$$

Or, quelque soit l'ensemble a, il n'y a pas d'ensemble satisfaisant la formule $(v_0 \in a \land \neg v_0 \simeq v_0)$. Il y a donc un ensemble qui ne possède aucun élément (parce que l'univers n'est pas vide). Par extensionnalité, il n'y en a qu'un seul, qui ne dépend donc pas de l'ensemble a. Cet ensemble est appelé l'**ensemble vide** et il est noté $\emptyset$.

Soient maintenant deux ensembles a et b. Le schéma de compréhension (avec $F[v_0,v_1] = v_0 \in v_1$ et en prenant $v_2 = a$, $v_1 = b$) permet de montrer l'existence d'un ensemble c tel que :

$$\forall v_0 (v_0 \in c \Longleftrightarrow (v_0 \in a \land v_0 \in b)).$$

L'unicité est, comme d'habitude, assurée par l'axiome d'extensionnalité. Cet ensemble c, dont les éléments sont donc exactement les ensembles appartenant à la fois à a et à b, est appelé l'**intersection de a et b** et noté $a \cap b$.

Soit a un ensemble non vide. Alors il existe un unique ensemble b dont les éléments sont les ensembles qui appartiennent à tous les éléments de a :

$$\forall v_0 (v_0 \in b \Longleftrightarrow \forall v_3 (v_3 \in a \Longrightarrow v_0 \in v_3)).$$

Pour montrer l'existence d'un tel ensemble (l'unicité découle de l'extensionnalité), on choisit un élément c de a (a n'est pas vide) et on remarque que la formule $\forall v_3 (v_3 \in a \Longrightarrow v_0 \in v_3)$ est équivalente à la formule $v_0 \in c \land \forall v_3 (v_3 \in a \Longrightarrow v_0 \in v_3)$. On applique alors le schéma de compréhension avec $F = \forall v_3 (v_3 \in v_1 \Longrightarrow v_0 \in v_3)$ et en prenant $v_2 = c$ et $v_1 = a$.

On note $\bigcap_{x \in a} x$, ou plus simplement $\bigcap a$ cet ensemble. Avec ces notations, on voit que :

$$\bigcap \{a\} = a \ , \ \bigcap \{a,b\} = a \cap b \ ,$$

et pour tout entier intuitif n,

$$\bigcap \{a_1, a_2, \ldots, a_n\} = a_1 \cap a_2 \ldots \cap a_n .$$

On remarque que la restriction «a non vide» est essentielle : en effet, la formule

$$\forall v_2 (v_2 \in \emptyset \Longrightarrow v_1 \in v_2)$$

est vérifiée par tous les ensembles (puisque $v_2 \in \emptyset$ n'est jamais vraie), et on a vu qu'il n'existait pas d'ensemble de tous les ensembles.

Si a et b sont des ensembles, on note a - b l'ensemble des éléments de a qui n'appartiennent pas à b :

$$a - b = \{x \in a \ ; \ x \notin b\}.$$

Si b est inclus dans a, a - b est appelé le **complémentaire** de b dans a.

On définit aussi la **différence symétrique de deux ensembles** :

$$a \, \Delta \, b = (a - b) \cup (b - a) .$$

REMARQUE : Les propriétés d'associativité, de commutativité ou de distributivité des connecteurs $\wedge$ et $\vee$ montrent que les propriétés correspondantes sont vraies pour $\cap$ et $\cup$. Par exemple :

$$a \cap b = b \cap a \ ; \ (a \cap b) \cap c = a \cap (b \cap c) \ ;$$
$$a \cup b = b \cup a \ ; \ (a \cup b) \cup c = a \cup (b \cup c) \ ;$$
$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c) \ ; \ a \cup (b \cap c) = (a \cup b) \cap (a \cup c) \, .$$

(Voir l'exercice 2 du chapitre 2.)

1.6 • **Le schéma d'axiome de remplacement.** Ce sont toutes les formules de la forme suivante :

$$\forall v_0 \forall v_1 \ldots \forall v_n (\forall w_0 \forall w_1 \forall w_2 ((F[w_0,w_1,v_1,v_2,\ldots,v_n] \wedge F[w_0,w_2,v_1,v_2,\ldots,v_n]) \Longrightarrow w_1 \simeq w_2) \Longrightarrow$$
$$\exists v_{n+1} \forall v_{n+2} (v_{n+2} \in v_{n+1} \Longleftrightarrow \exists w_0 (w_0 \in v_0 \wedge F[w_0,v_{n+2},v_1,v_2,\ldots,v_n]))) \, .$$

où n est un entier et $F[w_0,w_1,v_1,v_2,\ldots,v_n]$ une formule de $\mathscr{L}$.

Ces formules méritent quelques explications. Tout d'abord, donnons une définition :

DEFINITION : *On dit qu'une formule* $F[w_0,w_1,a_1,a_2,\ldots,a_n]$ *de* $\mathscr{L}$ *à deux variables libres et à paramètres dans* $\mathscr{U}$ ***est fonctionnelle en*** w_0 ***dans*** $\mathfrak{U}$ *si la formule suivante est vérifiée :*

$$\forall w_0 \forall w_1 \forall w_2 ((F[w_0,w_1,a_1,a_2,\ldots,a_n] \wedge F[w_0,w_2,a_1,a_2,\ldots,a_n]) \Longrightarrow w_1 \simeq w_2).$$

La plupart du temps, on omettra de préciser « dans $\mathscr{U}$ ». Si $F[w_0,w_1]$ est une formule fonctionnelle en w_0, elle permet de définir une fonction partielle (intuitive), que nous appellerons φ_F, de $\mathscr{U}$ dans $\mathscr{U}$: si b est un ensemble et s'il n'existe pas d'ensemble c telle que $F[b,c]$, alors φ_F n'est pas définie en b ; s'il en existe un, alors il en existe un seul, et $\varphi_F(b)$ est par définition cet ensemble.

Le schéma de remplacement affirme donc que si $F[w_0,w_1]$ est une formule fonctionnelle en w_0 (les variables $v_1,v_2,\ldots,v_n$ sont à remplacer par des paramètres de $\mathscr{U}$), et si a est un ensemble, alors la classe des images par φ_F des éléments de a est en fait un ensemble. On notera $\{x \ ; \ \exists v_0 \in a \ F[v_0,x]\}$ cet ensemble.

Il n'est pas très difficile de voir que le schéma de remplacement implique le schéma de compréhension. Soient $F[v_0,a_1,a_2,\ldots,a_n]$ une formule de $\mathscr{L}$ à paramètres dans $\mathscr{U}$ et b un ensemble. Montrons à l'aide du schéma de remplacement qu'il existe un ensemble c dont les éléments sont exactement les éléments de b satisfaisant $F[v_0,a_1,a_2,\ldots,a_n]$. On considère la formule :

$$H[w_0,w_1,a_1,a_2,\ldots,a_n] = w_0 \simeq w_1 \wedge F[w_0,a_1,a_2,\ldots,a_n].$$

Cette formule est évidemment fonctionnelle en w_0 et l'ensemble des images des éléments de b par φ_H est l'ensemble cherché.

Les autres axiomes ne seront énoncés qu'un peu plus loin.

Couples, relations et applications

1.7 DEFINITION 1 : *Soient* a *et* b *deux ensembles. L'ensemble*

$$\{\{a\},\{a,b\}\}$$

est appelé **couple** a,b *et est noté* (a,b).

C'est l'axiome de la paire, appliqué trois fois, qui permet d'affirmer que (a,b) est un ensemble. Cette définition un peu compliquée trouve sa justification dans la proposition suivante (d'ailleurs, toute autre définition conduisant à la même propriété aurait aussi bien convenu) :

PROPOSITION : *Soient* a, b, a' *et* b' *des ensembles et supposons que* (a,b) = (a',b'). *Alors* a = a' *et* b = b'.

☹ Par hypothèse, on a :

$$\{\{a\},\{a,b\}\} = \{\{a'\},\{a',b'\}\}.$$

On distingue deux cas :

1°) $a = b$; alors $\{\{a'\},\{a',b'\}\} = (a,b) = \{\{a\}\}$, et par conséquent :

$\{a',b'\} \in \{\{a\}\}$.

La remarque faite en 1.2 après l'énoncé de l'axiome de la paire montre donc que $a = a' = b'$.

2°) $a \neq b$; alors $\{a'\} \neq \{a,b\}$ (sinon, comme précédemment, $a = a' = b$) ; donc $\{a'\} = \{a\}$ et $a' = a$ (en utilisant toujours la remarque 1.2). D'autre part $\{a,b\} = \{a',b'\}$ et $b = b'$.

☺

Cette proposition justifie le nom de **paire ordonnée** que l'on emploie quelquefois à la place de couple.

Si (a,b) est un couple, alors, par définition, sa **première projection** (on dit quelquefois **composante** ou **coordonnée**) est a et sa **seconde projection** est b.

DEFINITION 2 : *Soient* a *et* b *des ensembles. On appelle* **somme disjointe** *de* a *et* b *l'ensemble*

$$\{(x,\emptyset)\ ;\ x \in a\} \cup \{(y,\{\emptyset\})\ ;\ y \in b\}.$$

Nous noterons a $\dot{\cup}$ b *la somme disjointe de* a *et* b.

La somme disjointe est donc la réunion des deux ensembles $\{(x,\emptyset)\ ;\ x \in a\}$ et $\{(y,\{\emptyset\})\ ;\ y \in b\}$. Il faut considérer, intuitivement, que ces ensembles sont des copies de a et b respectivement. L'intérêt de ces copies, c'est qu'elles sont nécessairement disjointes (c'est-à-dire que leur intersection est vide), ce qui n'est pas toujours le cas pour a et b.

NOTATION : On écrira **0** au lieu de $\emptyset$ et 1 au lieu de $\{\emptyset\}$. Ces notations seront justifiées par la suite.

1.8 PROPOSITION : *Soient* a *et* b *deux ensembles. Alors il existe un ensemble* c *tel que :*

$$\forall v_0(v_0 \in c \Longleftrightarrow \exists v_1 \exists v_2(v_1 \in a \wedge v_2 \in b \wedge v_0 \simeq (v_1,v_2))).$$

Autrement dit, étant donnés deux ensembles a et b, il existe un ensemble c dont les éléments sont les couples dont la première projection appartient à a et la seconde appartient à b. Cet ensemble est appelé le **produit cartésien** de a et de b et est noté a × b.

☺ Il suffit de voir que

$$c = \{u \in \mathfrak{P}(\mathfrak{P}(a \cup b))\ ;\ \exists v_0 \exists v_1(v_0 \in a \wedge v_1 \in b \wedge u \simeq (v_0,v_1))\}.$$

On utilise donc l'axiome de l'union, l'axiome des parties et un axiome de compréhension.
☺

Si a, b et c sont des ensembles, le **triplet** (a,b,c) est, par définition, l'ensemble (a,(b,c)). Plus généralement, si n est un entier intuitif strictement positif, on définit par récurrence la notion de **n–uplet** (ou **n-uple**) : si a_1, a_2, ..., a_n sont des ensembles, le n-uplet $(a_1,a_2,...,a_n)$ est l'ensemble $(a_1,(a_2,a_3,...,a_n))$; a_1 est la première projection de ce n-uplet, a_2 la deuxième etc. On voit comme ci-dessus que, si b_1, b_2, ..., b_n sont des ensembles, il existe un ensemble dont les éléments sont les n-uplets dont la première projection appartient à b_1, la deuxième à b_2, etc., et cet ensemble est noté

$b_1 \times b_2 \times \ldots \times b_n$. Si tous les b_i, pour i compris entre 1 et n, sont égaux à b, on écrira b^n au lieu de $b \times b \times \ldots \times b$ et on parlera de **puissance cartésienne** au lieu de produit cartésien.

1.9 DEFINITIONS :

1°) Soient a *un ensemble et* n *un entier (intuitif) strictement positif ; une* **relation** n**-aire** *sur* a *est un sous- ensemble de* a^n.

2°) Si n *est un entier, et* R *une relation* n*-aire sur* a *et* b *un sous ensemble de* a, *la* **restriction** *de* R *à* b *est l'ensemble* $R \cap b^n$ *; on note cette restriction* $R \restriction_b$.

3°) Une **application** *est un ensemble dont tous les éléments sont des couples et qui vérifie la formule suivante :*

$$App(v_0) = \forall v_1 \forall v_2 \forall v_3(((v_1,v_2) \in v_0 \wedge (v_1,v_3) \in v_0) \Longrightarrow v_2 \simeq v_3).$$

Si f *est une application, alors le* **domaine de définition** *de* f *(ou, plus simplement, le domaine de* f*), noté* $dom(f)$, *est l'ensemble des ensembles vérifiant la formule* $F[v_0] = \exists v_1 \, (v_0,v_1) \in f$. *L'***image de** f *est l'ensemble des ensembles vérifiant la formule* $G[v_0] = \exists v_1 \, (v_1,v_0) \in f$. *Une* **application de** a **dans** b *est une application dont le domaine est* a *et dont l'image est incluse dans* b. *Elle est* **surjective de** a **sur** b *si, de plus, son image est égale à* b. *Elle est* **injective** *si, pour tout* b *appartenant à l'image de* f, *il y a un unique élément* a *tel que* $(a,b) \in f$.

Il faut une petite justification à la définition de domaine de définition de f et de l'image de f : il faut montrer que ce sont des ensembles. Par exemple, le domaine de définition de f est l'ensemble :

$$\{x \in \bigcup \bigcup f \, ; \exists v_1 \, (x,v_1) \in f\}.$$

Insistons un peu : une application est donc un ensemble de couples. En revanche, on continuera d'employer le mot fonction dans le sens intuitif, et on pourra parler, par exemple, de fonction de l'univers $\mathcal{U}$ dans $\mathcal{U}$.

On peut continuer à traduire dans le langage de la théorie des ensembles toutes les notions usuelles concernant les applications. On se contentera de donner les définitions suivantes :

• Si f est une application et si a appartient au domaine de f, alors on note $f(a)$ l'unique ensemble b tel que $(a,b) \in f$. On l'appelle l'**image de** a **par** f.

• L'ensemble vide est une application dont le domaine et l'image sont tous les deux égaux à l'ensemble vide. Pour tout ensemble b, $\emptyset$ est donc une application de $\emptyset$ dans b. On parlera d'**application vide**.

• Si f est une application de a dans b et si g est une application de b dans c, alors **l'application composée** gof est l'ensemble :

$$\{u \in a \times c \ ; \exists v_0 \exists v_1 \exists v_2 (u \simeq (v_0,v_2) \land (v_0,v_1) \in f \land (v_1,v_2) \in g)\}.$$

C'est une application de a dans c.

• Une **bijection** de a sur b est une application surjective de a sur b qui est aussi injective. Si f est une bijection de a sur b, **l'application réciproque** f^{-1}, définie par :

$$f^{-1} = \{ (v_0,v_1) \in b \times a \ ; (v_1,v_0) \in f \}$$

est une bijection de b sur a.

• Si f est une application de a dans b et si c est une partie de a, on notera

$$\bar{f}(c) = \{ x \in b \ ; \exists y \in a\ f(y) \simeq x \} \ ;$$

$\bar{f}(c)$ est appelé l'**image directe** de c par f (on se contentera de parler d'image de c par f à ne pas confondre avec l'image de f, qui est l'image de a par f). Lorsqu'aucune confusion n'est à craindre, on écrira f(c) au lieu de $\bar{f}(c)$.

Dans les mêmes conditions, si d est une partie de b, on définit l'**image inverse** ou **image réciproque** de d par f :

$$\bar{f}^{-1}(d) = \{ x = a \ ; f(x) \in c \}$$

Ainsi, on peut associer à toute application de a dans b une application de $\mathfrak{P}(a)$ dans $\mathfrak{P}(b)$ et une application de $\mathfrak{P}(b)$ dans $\mathfrak{P}(a)$.

• Soient a et b deux ensembles. L'**exponentiation de a par b**, notée a^b (lire a puissance b) est l'ensemble des applications de b dans a.

Cette définition exige une justification : il faut montrer qu'il s'agit bien d'un ensemble. On utilise encore la compréhension : a^b est l'ensemble des éléments de $\mathfrak{P}(b \times a)$ qui satisfont la formule $F[v_0] = \forall v_1(v_1 \in b \Longrightarrow \exists! v_2\ (v_1,v_2) \in v_0)$.

• Soit I un ensemble ; une **famille d'ensembles indexée par** I est une application de domaine I.

Cette notion, d'usage courant, n'est introduite que parce qu'elle conduit à un langage et à des notations plus commodes. Si a est une famille indexée par I et si $i \in I$, on écrit généralement a_i au lieu de a(i) ; la famille a elle-même est notée $(a_i \ ; i \in I)$ ou, mieux, $(a_i)_{i \in I}$.

• Soit $a = (a_i)_{i \in I}$ une famille d'ensembles ; la **réunion** de cette famille, notée $\bigcup_{i \in I} a_i$, est la réunion des éléments de l'image de a. Autrement dit :

pour tout ensemble b, $b \in \bigcup_{i \in I} a_i$ si et seulement si il existe $i \in I$ tel que $b \in a_i$.

Si I n'est pas vide (cette restriction est essentielle, voir 1.5), on définit de même l'intersection de la famille $(a_i)_{i \in I}$, que l'on note $\bigcap_{i \in I} a_i$:

pour tout ensemble b, $b \in \bigcap_{i \in I} a_i$ si et seulement si, pour tout $i \in I$, $b \in a_i$.

• Soit encore $a = (a_i)_{i \in I}$ une famille d'ensemble. Le **produit** de cette famille, que l'on note $\prod_{i \in I} a_i$, est l'ensemble des applications f de I dans $\bigcup_{i \in I} a_i$ qui sont telles que, pour tout $i \in I$, $f(i) \in a_i$.

1.10 On peut maintenant énoncer l'**axiome du choix** : le produit d'une famille d'ensembles non vides est non vide ; autrement dit :

(AC) Soit $(a_i)_{i \in I}$ une famille d'ensembles et on suppose que, pour tout $i \in I$, a_i n'est pas vide. Alors $\prod_{i \in I} a_i$ n'est pas vide.

Nous ne discuterons pas la question de savoir si cet axiome est justifié ou non. Ce qui est sûr, mais qui ne sera pas démontré dans ce livre, c'est qu'il ne peut pas se déduire de la théorie ZF, pas plus d'ailleurs que sa négation (du moins si ZF est consistant) (voir 5.8). Par ailleurs il est nécessaire pour montrer certains théorèmes importants de mathématiques (par exemple : existence d'une base dans un espace vectoriel, théorème de Hahn-Banach (voir « analyse fonctionnelle » par L. Kantorovitch et G. Akilov, tome 1, MIR, éditions de Moscou), théorème de Krull (voir chapitre 2, 1.2)).

2. LES ORDINAUX ET LES ENTIERS

Ensembles bien ordonnés

2.1 Dans cette section, on va introduire la notion d'ordinal : c'est un outil particulièrement important en théorie des ensembles et en mathématiques en général. Elle peut être considérée comme une généralisation de la notion d'entier. On commence par quelques définitions.

DEFINITION : *Soient* X *un ensemble et* R *une relation binaire sur* X. *On dit que* R *est une* ***relation d'ordre*** *sur* X *(ou que* X ***est ordonné par*** R) *si :*

- *elle est transitive : si* $(x,y) \in R$ *et* $(y,z) \in R$, *alors* $(x,z) \in R$;
- *elle est antiréflexive : pour tout* $x \in X$, $(x,x) \notin R$.

On dit que R *est une* ***relation d'ordre total*** *(ou que* X ***est totalement ordonné par*** R*) si, en outre :*

- *pour tous* x, y *appartenant à* X, *si* x *et* y *sont distincts, alors* $(x,y) \in R$ *ou* $(y,x) \in R$.

Un ***ensemble (totalement) ordonné*** *est un couple* (X,R) *où* R *est une relation d'ordre (total) sur* X.

Les relations d'ordre que nous considérerons dans ce chapitre sont donc strictes, (c'est généralement le contraire dans le reste de ce livre). L'antisymétrie (pour tous x et y appartenant à X, $(x,y) \notin R$ ou $(y,x) \notin R$) se déduit de la transitivité et de l'antiréflexivité : si (x,y) et (y,x) appartenaient tous les deux à R, alors, par transitivité, (x,x) appartiendrait aussi à R, ce qui est impossible par antiréflexivité. On utilisera le langage habituel : si R est une relation d'ordre sur X et si x et y sont des points de X, on dira que x est **inférieur à** y **pour** R pour dire que $(x,y) \in R$, et on écrira $x <_R y$; on utilisera aussi les notations $x >_R y$, $x \leqslant_R y$ et $x \geqslant_R y$. On se permettra de ne pas mentionner R lorsqu'aucune ambiguïté n'est possible. Si (X,R) et (Y,S) sont deux ensembles ordonnés, un **isomorphisme** de (X,R) sur (Y,S) est une application f bijective de X sur Y qui satisfait : pour tous x, y dans X, $x <_R y$ si et seulement si $f(x) <_S f(y)$.

Si R est une relation d'ordre sur X et si Y est un sous-ensemble de X, alors un **élément minimum** (ou **plus petit élement**) de Y (pour R) est un élément de Y qui est inférieur ou égal à tous les éléments de Y ; un **élément minimal** de Y est un élément de Y qui n'est supérieur à aucun autre élément de Y (il n'y a pas de différence entre ces deux

notions si R est un ordre total). On définit de façon analogue un élément **maximum** et un élément **maximal**. Il y a au plus un élément minimum (ou maximum) mais il peut y avoir plusieurs éléments minimaux (ou maximaux). Un **minorant de** Y est un élément de X qui est inférieur ou égal à tous les éléments de Y ; une **borne inférieure de** Y est un élément maximal de l'ensemble des minorants de Y. Lorsque l'ordre est total, il y a au plus une borne inférieure. On définit de même un **majorant de** Y et une **borne supérieure** de Y.

Supposons maintenant que X soit totalement ordonné par R. Un **segment initial** de X est un sous-ensemble Y de X possédant la propriété suivante : si $y \in Y$ et $x <_R y$, alors $x \in Y$. Par exemple, X lui-même est un segment initial de X ; un **segment initial propre** de X est un segment initial de X différent de X et de l'ensemble vide . Si $x \in X$ et si x n'est pas l'élément minimum de X, l'ensemble

$$S_x = \{y \in X ; y <_R x\}$$

est un segment initial propre de X.

On remarque :

(1) Si Y est un segment initial de X et si x est un élément de X, alors on a $S_x \subsetneq Y$ (si $x \in Y$) ou $Y \subseteq S_x$ (si $x \notin Y$) ; en effet, si $x \in Y$, il est clair que $S_x \subsetneq Y$; sinon, pour tout élément y de Y, on ne peut avoir $x \leqslant y$ (car cela implique $x \in Y$), donc $Y \subseteq S_x$.

(2) L'ensemble des segments initiaux de X est totalement ordonné par la relation $\subsetneq$: en effet, si Y et Z sont deux segments initiaux de X, et s'il existe un élément x de Z tel que $x \notin Y$, on a, d'après (1) :

$$Y \subseteq S_x \subsetneq Z,$$

et donc $Y \subsetneq Z$; dans le cas contraire, $Z \subseteq Y$.

(3) L'ensemble des segments initiaux de X ainsi ordonné admet un plus petit élément (l'ensemble vide) et un plus grand élément (X lui-même).

2.2 DEFINITION 1 : *Soient* X *un ensemble et* R *une relation binaire sur* X. *On dit que* R *est une* ***relation de bon ordre***, *ou que* R *est un* ***bon ordre*** *sur* X, *ou encore que* X *est* ***bien ordonné*** *par* R *si :*

1°) R est une relation d'ordre total sur X.

2°) tout sous-ensemble non vide de X *admet un élément minimum.*

(On peut remarquer que la première condition peut être remplacée par : R est une relation d'ordre sur X ; en effet, si x et y sont des éléments distincts de X, alors $x \leqslant_R y$ ou $y \leqslant_R x$ suivant que l'élément minimum de $\{x,y\}$ est x ou y.) Comme exemple intuitif de bon ordre, il y a tous les ensembles finis totalement ordonnés et l'ensemble des entiers munis de la relation d'ordre habituelle. On va voir qu'il y en a bien d'autres.

Soit X un ensemble bien ordonné par une relation R. On remarque d'abord que, si Y est un sous-ensemble de X, alors $R\restriction_Y$ est un bon ordre sur Y. Si X n'est pas vide, il admet un élément minimum x_0 (on dira un premier élément). Si X n'est pas égal à $\{x_0\}$, alors $X - \{x_0\}$, l'ensemble des éléments de X différents de x_0, admet lui aussi un élément minimum, x_1, le « deuxième élément » de X ; on peut continuer ainsi.

Un autre propriété des ensembles bien ordonnés est la suivante :

PROPOSITION : *Soient* X *un ensemble bien ordonné et* Y *un segment initial de* X. *Alors soit* $Y = X$, *soit il existe un (unique) élément* x *de* X *tel que* $Y = S_x$.

☹ Supposons $Y \neq X$ et considérons l'élément minimum de $X - Y$, que nous appellerons x. On montre que $Y = S_x$: si $y \in Y$, alors $y < x$ (sinon $x \leqslant y$ et $x \in Y$), et donc $y \in S_x$. Si $z \in S_x$, alors $z < x$, et, parce que x est minimum dans $X - Y$, $z \in Y$.
☺

DEFINITION 2 : *Soit* X *un ensemble. On dit que* X *est* ***transitif*** *si tout élément de tout ensemble appartenant à* X *appartient à* X *(autrement dit, si la formule*

$$\forall v_0 \forall v_1((v_0 \in X \wedge v_1 \in v_0) \Longrightarrow v_1 \in X)$$

est satisfaite).

Un ensemble X est donc transitif si et seulement si tout ensemble appartenant à X est inclus dans X. Cette condition est encore équivalente à : $\bigcup X \subseteq X$.

Les ordinaux

2.3 DEFINITION : *Soit* α *un ensemble. On dit que* α *est un* ***ordinal*** *si les propriétés suivantes sont satisfaites :*

1°) α est transitif ;

2°) la relation d'appartenance sur α est une relation de bon ordre

(c'est-à-dire que l'ensemble $\{(x,y) \in \alpha \times \alpha\ ;\ x \in y\}$ *est une relation de bon ordre sur* α.*)*

Ces propriétés peuvent évidemment se traduire par des formules de $\mathscr{L}$. On notera $On[v_0]$ la formule de $\mathscr{L}$ exprimant que v_0 est un ordinal. Si α et β sont des ordinaux, on écrira indifféremment $\alpha \in \beta$ ou $\alpha < \beta$ (cette dernière notation, qui sera complètement justifiée en 2.6, conduit naturellement aux notations $\alpha \leqslant \beta$, $\alpha > \beta$, $\alpha \geqslant \beta$).

REMARQUE 1 : Si α est un ordinal, alors $\alpha \notin \alpha$, parce que l'appartenance, sur les éléments de α est une relation d'ordre (strict) : si on suppose que α appartient à α, on en déduit que α n'appartient pas à α.

REMARQUE 2 : Si α est un ordinal et si $\beta \in \alpha$, alors β est un ordinal. Puisque α est transitif, $\beta \subseteq \alpha$, et donc la relation d'appartenance sur β, qui est égale à la relation d'appartenance sur α restreinte à β, est une relation de bon ordre. Il reste à voir que β est transitif : si $\gamma \in \beta$ et $\delta \in \gamma$, alors β ,γ , δ sont des éléments de α (parce que α est transitif), et, par transitivité de la relation $\in$ sur α, $\delta \in \beta$.

REMARQUE 3 : Si α est un ordinal et si $\beta \in \alpha$, alors $\beta = S_\beta$: c'est une conséquence de l'axiome d'extensionnalité, puisqu'il est équivalent de dire que $x \in \beta$ ou que $x \in S_\beta$.

REMARQUE 4 : Soient α et β deux ordinaux. Alors $\alpha \subseteq \beta$ si et seulement si $\alpha \leqslant \beta$. En effet, si α est inclus dans β, alors, parce que α est transitif, α est un segment initial de β. Donc, soit $\alpha = \beta$, soit il existe $\gamma \in \beta$ tel que $\alpha = S_\gamma$ (proposition 2.2), et (remarque 3) $\alpha = \gamma$, donc $\alpha < \beta$. Réciproquement, si $\alpha \leqslant \beta$ (c'est-à-dire $\alpha \in \beta$ ou $\alpha = \beta$), et si $\gamma \in \alpha$, alors par transitivité de β, $\gamma \in \beta$; cela montre que $\alpha \subseteq \beta$.

PROPOSITION : *Soit* X *un ensemble transitif d'ordinaux tel que, pour tous éléments* x *et* y *de* X, $x \in y$ *ou* $y \in x$ ou $x = y$; *alors* X *est un ordinal.*

(On verra un peu plus loin (corollaire 2.5) que la condition « $x \in y$ ou $y \in x$ ou $x = y$ » est superflue parce qu'elle est toujours satisfaite.)

☺ Il suffit de vérifier la seconde condition de la définition 2.3. Si $\alpha \in X$, alors $\alpha \notin \alpha$ (remarque 1). Si α, β et γ sont des éléments de X et si $\alpha \in \beta$ et $\beta \in \gamma$, alors la transitivité

de γ implique que $\alpha \in \gamma$. L'appartenance définit bien une relation d'ordre sur X, et cet ordre est total par hypothèse.

Montrons qu'il s'agit d'un bon ordre : soit Y un sous-ensemble non vide de X ; on va voir que Y admet un élément minimum (pour $\in$) ; soit $\alpha \in Y$:

– si $\alpha \cap Y = \emptyset$, alors α est l'élément minimum de Y : si $\beta \in Y$, il est faux que $\beta \in \alpha$ (parce que $\alpha \cap Y = \emptyset$) et donc $\alpha \in \beta$ ou $\alpha = \beta$;

– si $\alpha \cap Y \neq \emptyset$, alors, parce que α est un ordinal, $\alpha \cap Y$ admet un élément minimum β ; si $\gamma \in \beta$, alors $\gamma \in \alpha$ (α est un ordinal) et $\gamma \notin \alpha \cap Y$ (β est minimum dans $\alpha \cap Y$). Par conséquent, $\gamma \notin Y$, et donc, aucun élément de Y ne peut être strictement inférieur à β. Puisque l'ordre est total, cela implique que β est l'élément minimum de Y.
☺

COROLLAIRE 1 : *Si α est un ordinal et si β est un segment initial de α, alors β est un ordinal ; si, de plus, β est un segment initial propre de α, alors $\beta \in \alpha$.*

☹ La première partie découle de la proposition ci-dessus : β est transitif parce que c'est un segment initial de α, et β est totalement ordonné par $\in$ parce que α l'est.

Supposons de plus que β ne soit pas égal à α ; par la proposition 2.2, il existe $\gamma \in \alpha$ tel que $\beta = S_\gamma$, et par la remarque 3, $\gamma = S_\gamma$.
☺

L'ensemble vide est manifestement un ordinal. C'est même le plus petit de tous les ordinaux : si α est un ordinal non vide, alors $\emptyset \in \alpha$: en effet α contient un élément minimum, que l'on appellera β. Tous les éléments de β appartiennent aussi à α (parce que α est transitif), et sont strictement inférieurs à β, ce qui est incompatible avec la minimalité de β : $\beta = \emptyset$.

L'ensemble $\{\emptyset\}$ est aussi un ordinal, comme cela se vérifie facilement sur la définition. Les ensembles suivants sont aussi des ordinaux :

$\{\emptyset, \{\emptyset\}\}$; $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

Plus généralement :

COROLLAIRE 2 : *Si α est un ordinal alors $\beta = \alpha \cup \{\alpha\}$ est aussi un ordinal.*

☹ On utilise encore la proposition ci-dessus. Montrons d'abord que β est un ensemble transitif : si $\gamma \in \beta$, et $\delta \in \gamma$ alors : soit $\gamma \in \alpha$, et $\delta \in \alpha$ parce que α est transitif ;

soit $\gamma = \alpha$ et évidemment $\delta \in \alpha$. Par ailleurs si x et y sont deux éléments distincts de β, alors : soit ils appartiennent tous les deux à α et on a bien $x \in y$ ou $y \in x$ parce que α est un ordinal ; soit l'un des deux est égal à α et l'autre appartient à α et on obtient la même conclusion.

☺

L'ordinal $\alpha \cup \{\alpha\}$ sera noté α^+ et sera appelé le successeur de α. On dit qu'un ordinal est **limite** s'il n'est pas égal à $\emptyset$ et s'il n'est pas le successeur d'un autre ordinal.

2.4 On en vient maintenant à un théorème un peu plus difficile, et dont les corollaires seront extrêmement importants. On va utiliser, sans le dire, les démonstrations et les définitions par induction. On fera une analyse plus précise et plus systématique de celles-ci à la section suivante.

THEOREME : *Soient* X *et* Y *deux ensembles bien ordonnés par les relations* R *et* S *respectivement. Alors au moins un des deux cas suivants se produit :*

a) il existe un et un seul segment initial Y_1 *de* Y *et un et un seul isomorphisme* f *de* (X,R) *sur* $(Y_1, S\restriction_{Y_1})$;

b) il existe un et un seul segment initial X_1 *de* X *et un et un seul isomorphisme* g *de* (Y,S) *sur* $(X_1, R\restriction_{X_1})$.

De plus, si a) et b) ont lieu simultanément, alors $X_1 = X$, $Y_1 = Y$ *et les applications* f *et* g *sont inverses l'une de l'autre.*

☹ Dans cette preuve, on va considérer des segments initiaux de X et de Y. On les considérera toujours comme des ensembles ordonnés par la restriction de R ou de S. Lorsqu'on parlera d'isomorphisme entre de tels ensembles, il s'agira toujours d'isomorphisme d'ensembles ordonnés.

On montre d'abord l'unicité. Supposons par exemple que Y_1 et Y_2 soient deux segments initiaux de Y et que f_1 et f_2 soient des isomorphismes de X sur Y_1 et Y_2, respectivement. Considérons l'ensemble :

$$Z = \{x \in X \; ; \; f_1(x) \neq f_2(x)\}.$$

On va montrer que Z est vide. Raisonnons par l'absurde : si Z n'est pas vide, il existe un élément minimum x_0 (pour R) dans Z. Supposons par exemple que $f_1(x_0) <_S f_2(x_0)$. Comme Y_2 est un segment initial de Y, $f_1(x_0) \in Y_2$, et il existe $x_1 \in X$ tel que

$$f_2(x_1) = f_1(x_0) <_S f_2(x_0).$$

Puisque f_2 est un isomorphisme, $x_1 <_R x_0$. Or x_0 a été choisi minimum dans Z, donc $f_1(x_1) = f_2(x_1)$, d'où il découle que $f_1(x_1) = f_1(x_0)$, contredisant le fait que f_1 est injective.

L'unicité en b) se démontre de la même façon. Supposons maintenant que a) et b) aient lieu simultanément. On voit facilement que $g(Y_1)$ est un segment initial de X, et donc $g \circ f$ est un isomorphisme de X dans un de ses segments initiaux. Or, l'application identique sur X est aussi un isomorphisme de X sur un de ses segments initiaux (à savoir X lui-même), et en appliquant l'unicité déjà démontrée (appliquée au cas où $Y = X$ et $S = R$), on voit que $g \circ f$ est égale à l'application identique sur X. Comme f et g sont injectives, on en déduit qu'elles sont inverses l'une de l'autre.

Il reste à montrer l'existence. Considérons les ensembles :

$A = \{(x,y) \in X \times Y$; il existe un isomorphisme de S_x sur $S_y\}$

et $A^* = \{(y,x) \in Y \times X$; il existe un isomorphisme de S_x sur $S_y\}$

Supposons que (x,y) et (x,z) appartiennent tous les deux à A ; il existe donc deux isomorphismes de S_x sur S_y et S_z respectivement, qui sont des segments initiaux de Y. On vient de voir que cela implique : $S_y = S_z$, donc $y = z$. Autrement dit, A est une application dont le domaine, que nous appellerons A_1, est inclus dans X et dont l'image, que nous appellerons A_2 est incluse dans Y. On montre de même que A^* est une application, et comme $(x,y) \in A$ si et seulement si $(y,x) \in A^*$, on en conclut que le domaine de A^* est A_2, que son image est A_1, et que A et A^* sont des applications réciproques l'une de l'autre. Ce sont donc toutes les deux des bijections.

Une petite remarque : supposons que h soit un isomorphisme d'un ensemble totalement ordonné U sur un ensemble totalement ordonné V. Il est alors très facile de vérifier que, pour tout $u \in U$, l'image par h de l'ensemble $\{t \in U \ , \ t < u\}$ est égale à $\{v \in V \ ; \ v < h(u)\}$; autrement dit $\bar{h}(S_u) = S_{h(u)}$.

Ceci montre que A_1 est un segment initial de X : si $x \in A_1$ et $z <_R x$, alors il existe $y \in Y$ et un isomorphisme f de S_x sur S_y ; la restriction de f à S_z est un isomorphisme de S_z sur un segment initial de S_y, qui est aussi un segment initial de Y. De même A_2 est un segment initial de Y.

On voit aussi que A, non content d'être bijectif, est un isomorphisme : supposons en effet que (x,y) et (z,t) appartiennent à A et que $z <_R x$; il existe donc un isomorphisme f de S_x sur S_y, et $f\restriction_{S_z}$ est un isomorphisme de S_z sur un segment initial de Y qui, par l'unicité déjà prouvée, ne peut être que S_t : donc $t <_S y$.

Si $A_1 = X$, la conclusion du théorème est vraie parce que *a*) est vrai ; si $A_2 = Y$, alors c'est *b*) qui est vrai. Montrons par l'absurde qu'il n'est pas possible que $A_1 \neq X$ et $A_2 \neq Y$: par la proposition 2.2, il existerait $x \in X$ et $y \in Y$ tels que $A_1 = S_x$ et $A_2 = S_y$. Mais alors, A est un isomorphisme de S_x sur S_y, ce qui prouve que $(x,y) \in A$ et que $x \in A_1 = S_x$, ce qui est absurde.

☺

2.5 On va appliquer ce théorème au cas des ordinaux. On a déjà remarqué qu'un segment initial d'un ordinal est un ordinal (voir corollaire 1, 2.3). D'autre part :

PROPOSITION : *Soient α et β des ordinaux et* f *un isomorphisme de α sur β. Alors $\alpha = \beta$ et* f *est l'identité sur α.*

☹ Considérons l'ensemble :

$$X = \{x \in \alpha \,;\, f(x) \neq x\}.$$

Si cet ensemble n'est pas vide, il admet un plus petit élément, x_0. Examinons $f(x_0)$: si $y \in x_0$, alors $y \in \alpha$ (α est transitif) et $f(y) \in f(x_0)$ (f est un isomorphisme) ; par minimalité de x_0, $y = f(y)$. On en déduit : $x_0 \subseteq f(x_0)$.

Réciproquement, si $y \in f(x_0)$, alors $y \in \beta$ (β est transitif) et il existe $z \in \alpha$ tel que $y = f(z)$ (f est surjective sur β). Puisque f est un isomorphisme, $z \in x_0$, et par minimalité de x_0, $z = f(z) = y$. Donc $f(x_0) \subseteq x_0$ et, par extensionnalité, $x_0 = f(x_0)$. Nous avons obtenu une contradiction, donc X est vide et la proposition est démontrée.

☺

COROLLAIRE : *Soient α et β des ordinaux. Alors une et une seule des trois éventualités suivantes se produit :*

1°) $\alpha \in \beta$;

2°) $\beta \in \alpha$;

3°) $\alpha = \beta$.

☹ Il n'est pas possible que deux de ces éventualités se produisent en même temps : cela découle facilement de la remarque 1 de 2.3 et du fait que les ordinaux sont des ensembles transitifs.

On applique le théorème 2.4 ; supposons, par exemple qu'il existe un isomorphisme f de α sur un segment initial S de β. Si ce segment initial est propre, alors, d'après le corollaire 1 de 2.3, S est lui-même un ordinal et appartient à β. D'après la proposition 2.5, $S = \alpha$, et donc $\alpha \in \beta$. Sinon, f est un isomorphisme de α sur β, et on applique directement la proposition 2.5 pour obtenir $\alpha = \beta$. On fait un raisonnement analogue s'il existe un isomorphisme de β sur un segment initial de α.

☺

REMARQUE : La proposition 2.3 devient : tout ensemble transitif d'ordinaux est un ordinal.

2.6 On considère maintenant la classe des ordinaux (c'est-à-dire la classe des ensembles satisfaisant la formule $On[v_0]$). On s'apprête à montrer que cette classe n'est pas un ensemble. Cependant, l'appartenance sur cette classe possède les propriétés d'une relation de bon ordre :

- (transitivité) : Si α, β et γ sont des ordinaux et $\alpha \in \beta$ et $\beta \in \gamma$, alors $\alpha \in \gamma$ (parce que γ est un ensemble transitif) ;
- (antiréflexivité) : si α est un ordinal, alors $\alpha \notin \alpha$ (remarque 1 de 2.3) ;
- (totalité) : si α et β sont des ordinaux alors $\alpha \in \beta$ ou $\beta \in \alpha$ ou $\alpha = \beta$ (corollaire 2.5) ;
- Soit $F[v_0]$ une formule avec paramètres dans $\mathscr{U}$, et supposons qu'il existe des ordinaux satisfaisant $F[v_0]$. Alors, il y en a un plus petit ; plus précisément : il existe un ordinal α tel que $F[\alpha]$ soit vrai, et pour tout ordinal β, $F[\beta]$ implique $\alpha \in \beta$ ou $\alpha = \beta$. Pour montrer cela, on considère un ordinal γ satisfaisant $F[\gamma]$ (il en existe, par hypothèse). Alors l'ensemble :

$$\{\beta \in \gamma^+ : F[\beta]\}$$

n'est pas vide, puisqu'il contient γ, et possède donc un élément minimal puisque γ^+ est un ordinal. Cet élément minimal est l'ordinal cherché.

On dira que l'appartenance, sur la classe des ordinaux, est une méta-relation de bon ordre.

PROPOSITION 1 : *La classe des ordinaux n'est pas un ensemble.*

☹ Supposons le contraire, et appelons X l'ensemble de tous les ordinaux ; si $\alpha \in X$ et $\beta \in \alpha$, alors $\beta \in X$ (remarque 2 de 2.3). Ceci et la remarque 2.5 nous permet d'appliquer la proposition 2.3 : X est un ordinal, donc $X \in X$, ce qui contredit la remarque 1 de 2.3.

☺

PROPOSITION 2 : *Si* A *est un ensemble d'ordinaux, alors*

$$\beta = \bigcup_{\alpha \in A} \alpha$$

est un ordinal.

☹ Il est à peu près immédiat de vérifier que toute réunion d'ensembles transitifs est un ensemble transitif ; donc β est un ensemble transitif d'ordinaux ; il suffit encore d'appliquer la remarque 2.5.

☺

Considérons un ensemble A d'ordinaux et posons $\beta = \bigcup_{\alpha \in A} \alpha$. Supposons que α appartienne à A ; par définition de A et β, $\alpha \subseteq \beta$, et donc (remarque 4 de 2.3) $\alpha \leqslant \beta$. On voit ainsi que β est supérieur ou égal à tous les éléments de A. C'est même le plus petit des ordinaux supérieurs ou égaux à tous les éléments de A : si γ est supérieur ou égal à tous les éléments de A, alors, pour tout $\alpha \in A$, $\alpha \subseteq \gamma$, ce qui montre que $\beta \subseteq \gamma$, et, donc $\beta \leqslant \gamma$.

On voit donc que β est la borne supérieure de A. On notera $\beta = \bigcup_{\alpha \in A} \alpha = \sup A$.

PROPOSITION 3 : *Soit* X *un ensemble bien ordonné par une relation* R *; alors, il existe un et un seul ordinal* α *isomorphe à* (X,R). *De plus, il n'y a qu'un seul isomorphisme de* α *sur* (X,R).

☹ Les unicités ont déjà été prouvées au théorème 2.4. On raisonne par l'absurde. En appliquant le théorème 2.4, on voit que chaque ordinal α est isomorphe à un segment initial de X. Considérons l'ensemble :

$$T = \{x \in \mathfrak{P}(X) \ ; \ x \text{ est un segment initial de X et } x \text{ est isomorphe à un ordinal}\},$$

et la formule :

$$F[v_0,v_1] = v_0 \in T \wedge On[v_1] \wedge \text{il existe un isomorphisme de } v_0 \text{ dans } v_1.$$

Cette formule est fonctionnelle en v_0 (définition 1.6) (c'est encore une conséquence du théorème 2.4). Le schéma de remplacement permet donc d'affirmer que l'ensemble $O = \{\alpha \ ; \ \exists v_0 \in T \ F[v_0,\alpha]\}$ existe. Or, par hypothèse, pour tout ordinal α, il existe un isomorphisme de α sur un segment initial de X, et on a donc $\exists v_0(v_0 \in T \wedge F[v_0,\alpha])$. Autrement dit, O est l'ensemble de tous les ordinaux, ce qui est impossible d'après la proposition 1.

☺

REMARQUE : Soient α un ordinal et X un sous-ensemble de α ; on a vu que X est bien ordonné par $\in$. Par conséquent, il existe un ordinal β et un isomorphisme f de β sur X. Montrons que $\beta \leqslant \alpha$. Ceci découlera du lemme suivant :

LEMME : *Soit* f *une application strictement croissante d'un ordinal* β *dans un ordinal* α *; alors, pour tout ordinal* $\gamma \in \beta$, $f(\gamma) \geqslant \gamma$.

☹ On raisonne par l'absurde : soit γ le plus petit ordinal tel que $f(\gamma) < \gamma$. Pour tout $\delta \in \gamma$, $\delta \leqslant f(\delta)$, et, d'autre part, $f(\delta) < f(\gamma)$ (parce que f est strictement croissante); donc $\delta \in f(\gamma)$. Il en résulte donc que $\gamma \subseteq f(\gamma)$, et avec la remarque 4 de 2.3, $\gamma \leqslant f(\gamma)$.

☺

2.7 On introduit maintenant le dernier axiome de ZF, l'axiome de l'infini :

DEFINITION : *Soit α un ordinal. On dit que α est* ***fini*** *si, ni lui-même, ni aucun de ses éléments, n'est un ordinal limite. Un ordinal* ***infini*** *est un ordinal qui n'est pas fini.*

On remarque que si α est un ordinal fini et $\beta \in \alpha$, alors β est aussi un ordinal fini. Par exemple, $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$ sont des ordinaux finis. Plus généralement, si α est un ordinal fini, alors α^+ est aussi un ordinal fini. En fait, l'existence d'un ordinal infini nécessite l'introduction d'un nouvel axiome, naturellement appelé **axiome de l'infini** :
(Inf) il existe un ordinal infini.
Il équivaut clairement à : « il existe un ordinal limite » qui est la formule :

$$\exists v_0(On[v_0] \wedge \neg v_0 \simeq \emptyset \wedge \forall v_1 \neg v_0 \simeq v_1 \cup \{v_1\})$$

Conformément à ce que nous avons dit en 1.1, on suppose à partir de maintenant que cet axiome est vérifié dans $\mathfrak{U}$.

On verra à la dernière section que cet axiome ne peut pas se déduire des précédents.

NOTATION : *On note ω le plus petit des ordinaux infinis.*

Un tel ordinal existe, parce que la classe des ordinaux est une classe bien ordonnée (voir 2.6). Remarquons que ω est aussi l'ensemble des ordinaux finis : si α est un ordinal fini, alors aucun ordinal inférieur à α n'est infini et donc, $\alpha \in \omega$. Réciproquement, si $\alpha \in \omega$, alors, par minimalité de ω, α est fini.

Opérations sur les ordinaux

2.8 On va maintenant définir quelques opérations sur les ordres et les ordinaux.

• Soient $\mathfrak{a} = (a,R)$ et $\mathfrak{b} = (b,S)$ deux ensembles ordonnés. On va définir un nouvel ensemble ordonné, que l'on appellera la **somme directe de $\mathfrak{a}$ et $\mathfrak{b}$** et que l'on notera $\mathfrak{a} \oplus \mathfrak{b}$. L'ensemble de base de $\mathfrak{a} \oplus \mathfrak{b}$ est $a \,\dot\cup\, b$ (l'union disjointe de a et b) (voir 7. 2, définition 1). Posons $c = a \,\dot\cup\, b$. On définit sur cet ensemble la relation binaire T par :

Pour tous (x_0,y_0) et (x_1,y_1) dans c, $((x_0,y_0),(x_1,y_1)) \in T$ si et seulement :

$y_0 = 0$ et $y_1 = 1$;

ou $y_0 = y_1 = 0$ et $x_0 <_R x_1$;

ou $y_0 = y_1 = 1$ et $x_0 <_S x_1$.

Intuitivement, l'ensemble a ⊍ b est constitué d'un copie de a et d'une copie de b. Dans la relation que l'on vient de définir, les éléments de la copie de a sont ordonnés entre eux comme ils le sont dans 𝔞 et précèdent les éléments de la copie de b, qui, eux, sont ordonnés entre eux comme ils le sont dans 𝔟.

Il faut vérifier que la relation T est une relation d'ordre. Voyons la transitivité. Soient (x_0,y_0), (x_1,y_1) et (x_2,y_2) trois éléments de c, et on suppose que $((x_0,y_0),(x_1,y_1))$ et $((x_1,y_1),(x_2,y_2))$ appartiennent tous les deux à T. Il y a plusieurs cas possibles :

• $y_2 = 0$. Alors la définition de T implique que $y_0 = y_1 = 0$, $x_0 <_R x_1$ et $x_1 <_R x_2$. Par transitivité de R, on en déduit que $x_0 <_R x_2$, et donc que $((x_0,y_0),(x_2,y_2)) \in T$.

• $y_2 = 1$ et $y_0 = 0$. Alors $((x_0,y_0),(x_2,y_2)) \in T$, par définition de T.

• $y_0 = y_2 = 1$. Alors, $y_1 = 1$, $x_0 <_S x_1$ et $x_1 <_S x_2$. Par transitivité de S, on en déduit que $x_0 <_S x_2$, et donc que $((x_0,y_0),(x_2,y_2)) \in T$.

On laisse au lecteur le soin de montrer que T est antiréflexive, et aussi que T est une relation d'ordre total si R et S le sont.

Supposons de plus que 𝔞 et 𝔟 soient tous les deux des bons ordres. On va voir qu'il en est de même de 𝔞 ⊕ 𝔟. Soit d un sous-ensemble non vide de c. Il s'agit de montrer qu'il contient un élément minimum. De deux choses l'une : soit il existe des éléments x dans a tels que $(x,0) \in c$; dans ce cas, si x_0 est le plus petit de ces éléments, $(x_0,0)$ est l'élément minimum de c ; soit tous les éléments de d sont de la forme $(y,1)$, avec $y \in b$, et, en appelant y_0 le plus petit des éléments y de b tels que $(y,1) \in d$, $(y_0,1)$ est l'élément minimum de c.

Donc, si α et β sont des ordinaux, $\alpha \oplus \beta$ est un bon ordre, et par la proposition 3 de 2.6, il est isomorphe à un unique ordinal. D'où la définition :

DEFINITION : *Soient α et β des ordinaux. Alors l'unique ordinal isomorphe à $\alpha \oplus \beta$ est appelé* ***somme ordinale de α et β*** *et noté $\alpha + \beta$.*

2.9 • Passons maintenant au produit. Soient encore $\mathfrak{a} = (a,R)$ et $\mathfrak{b} = (b,S)$ deux ensembles ordonnés. On définit la relation T sur $c = a \times b$ par :

pour tous (x_0,y_0), (x_1,y_1) appartenant à c, $((x_0,y_0),(x_1,y_1)) \in T$ si et seulement si l'une des deux conditions suivantes est vérifiée : a) $y_0 <_S y_1$; b) $y_0 = y_1$ et $x_0 <_R x_1$.

Il faut encore vérifier que T est une relation d'ordre. Voyons la transitivité : soient (x_0,y_0), (x_1,y_1) et (x_2,y_2) trois éléments de c, et on suppose que $((x_0,y_0),(x_1,y_1))$ et $((x_1,y_1),(x_2,y_2))$ appartiennent tous les deux à T. Il découle de cela que $y_0 \leqslant_S y_1 \leqslant_S y_2$. Il

y a donc deux possibilités : ou bien $y_0 <_S y_2$, et alors, par définition de T, $((x_0,y_0),(x_2,y_2)) \in T$; ou bien $y_0 = y_1 = y_2$, et dans ce cas $x_0 <_R x_1 <_R x_2$, et on a encore $((x_0,y_0),(x_2,y_2)) \in T$.

Le lecteur vérifiera encore que T est antiréflexive et que T est une relation d'ordre total si R et S le sont. On notera $\mathfrak{a} \otimes \mathfrak{b}$ l'ensemble $a \times b$ ordonné par T.

Montrons comme précédemment que T est une relation de bon ordre si R et S le sont. Soit d un sous-ensemble non vide de $a \times b$. Alors l'ensemble

$$\{y \in b \text{ ; il existe } x \in a \text{ tel que } (x,y) \in d\}$$

est non vide. Soit y_0 son élément minimum, et x_0 l'élément minimum de l'ensemble

$$\{x \in a \text{ ; } (x,y_0) \in d\}.$$

Alors, on voit sans problème que (x_0,y_0) est l'élément minimum de d.

La définition suivante est donc justifiée :

DEFINITION : *Soient α et β deux ordinaux. Alors l'unique ordinal isomorphe à $\alpha \otimes \beta$ est appelé* **produit ordinal de α et β** *et noté $\alpha \times \beta$.*

2.10 THEOREME : *Soient α, β et γ des ordinaux. Alors :*

i) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$;

ii) $\alpha \times (\beta \times \gamma) = (\alpha \times \beta) \times \gamma$;

iii) $\alpha \times (\beta + \gamma) = (\alpha \times \beta) + (\alpha \times \gamma)$;

iv) $\alpha + 0 = \alpha = 0 + \alpha$;

v) $\alpha \times 0 = 0 \times \alpha = \emptyset$;

vi) $\alpha \times 1 = 1 \times \alpha = \alpha$;

vii) $\alpha^+ = \alpha + 1$;

viii) *si α et β sont finis, il en est de même de $\alpha + \beta$ et de $\alpha \times \beta$;*

ix) *si $\alpha^+ = \beta^+$, alors $\alpha = \beta$;*

x) *si α et β sont des ordinaux finis, alors $\alpha < \beta$ si et seulement si il existe un ordinal γ non nul tel que $\alpha + \gamma = \beta$.*

☹ Les démonstrations de *i)*, *ii)* et *iii)* reposent sur le même principe. Par exemple, pour *i)*, on démontre que si $\mathfrak{a} = (a,R)$, $\mathfrak{b} = (b,S)$ et $\mathfrak{c} = (c,T)$ sont trois ensembles ordonnés, alors $\mathfrak{a} \oplus (\mathfrak{b} \oplus \mathfrak{c})$ est isomorphe à $(\mathfrak{a} \oplus \mathfrak{b}) \oplus \mathfrak{c}$. Voici l'isomorphisme f de $\mathfrak{a} \oplus (\mathfrak{b} \oplus \mathfrak{c})$ sur $(\mathfrak{a} \oplus \mathfrak{b}) \oplus \mathfrak{c}$: si $x \in a \,\dot\cup\, (b \,\dot\cup\, c)$, alors :

- soit $x = (y,0)$ avec $y \in a$; dans ce cas, on pose : $f(x) = ((y,0),0)$;
- soit $x = ((y,0),1)$, avec $y \in b$; on pose alors : $f(x) = ((y,1),0)$;
- soit $x = ((y,1),1)$, avec $y \in c$; alors : $f(x) = (y,1)$.

Pour *ii)*, on montre, avec $\mathfrak{a}$, $\mathfrak{b}$ et $\mathfrak{c}$ comme ci-dessus, que $\mathfrak{a} \otimes (\mathfrak{b} \otimes \mathfrak{c})$ est isomorphe à $(\mathfrak{a} \otimes \mathfrak{b}) \otimes \mathfrak{c}$. L'isomorphisme f est défini par :

$$\text{pour tous } x \in a,\ y \in b \text{ et } z \in c,\ f((x,(y,z))) = ((x,y),z).$$

Pour *iii)*, il faut définir un isomorphisme f de $\mathfrak{a} \otimes (\mathfrak{b} \oplus \mathfrak{c})$ sur $(\mathfrak{a} \otimes \mathfrak{b}) \oplus (\mathfrak{a} \otimes \mathfrak{c})$. Le voici :

- si $x = (y,(z,0))$, avec $y \in a$ et $z \in b$, alors $f(x) = ((y,z),0)$;
- si $x = (y,(z,1))$, avec $y \in a$ et $z \in c$, alors $f(x) = ((y,z),1)$.

Les égalités *iv)* et *v)* sont à peu près évidentes ; *vi)* se déduit de l'isomorphisme f de α sur $\alpha \otimes 1$ défini par : pour tout $\beta \in \alpha$, $f(\beta) = (\beta,0)$. L'application f définie comme suit est un isomorphisme de α^+ sur $\alpha \oplus \{\emptyset\}$:

- si $\beta \in \alpha$, $f(\beta) = (\beta,0)$,
- $f(\alpha) = (\emptyset,1)$,

ce qui prouve *vii)*.

viii) Supposons maintenant que α et β sont des ordinaux finis, et supposons, en raisonnant par l'absurde, que $\alpha + \beta$ est infini. Considérons alors l'ensemble :

$$A = \{x \in \omega\ ;\ \alpha + x \text{ est infini}\}.$$

Cet ensemble, n'étant pas vide (β en est un élément), possède un élément minimum que nous appellerons x_0. On voit que $x_0 \neq \emptyset$ (parce que $\alpha + 0 = \alpha$ et que α est fini) ; comme x_0 est fini, il n'est pas limite, et il existe donc un ordinal y_0 tel que $y_0^+ = y_0 + 1 = x_0$. Alors $\alpha + x_0 = (\alpha + y_0) + 1 = (\alpha + y_0)^+$ (par *i)* et *vii)*), $\alpha + y_0$ est fini (parce que x_0 est l'élément minimum de A), et on a vu (voir le commentaire suivant la définition 2.7) que le successeur d'un ordinal fini est fini, donc $\alpha + x_0$ est aussi fini : contradiction.

La somme de deux ordinaux finis est donc un ordinal fini. Raisonnons encore par l'absurde pour prouver que le produit de deux ordinaux finis est fini : supposons que l'ensemble :

$$B = \{x \in \omega\ ;\ \alpha \times x \text{ est infini}\}$$

ne soit pas vide, et considérons-en l'élément minimum x_0. Par *v)*, on voit que x_0 n'est pas l'ensemble vide, et il existe donc un ordinal y_0 tel que $x_0 = y_0 + 1$. Par *iii)* et *vi)* on voit que $\alpha \times x_0 = (\alpha \times y_0) + \alpha$. Or, $\alpha \times y_0$ est fini, parce que x_0 est minimum dans B et α est fini par hypothèse, et on vient de voir qu'il en découle que $(\alpha \times y_0) + \alpha$ est fini : contradiction.

ix) Il est à peu près clair que α est l'élément maximum de α^+ (et β est l'élément maximum de β^+). Donc, si $\alpha^+ = \beta^+$ alors $\alpha = \beta$.

x) Il est clair que si γ est un ordinal non nul, $\alpha + \gamma \geqslant \alpha + 1 = \alpha^+ > \alpha$. Cela montre le sens « si ». Pour l'autre sens, on raisonne par l'absurde : soit β le plus petit ordinal fini tel que : $\beta > \alpha$ et il n'existe pas d'ordinaux γ tel que $\alpha + \gamma = \beta$. Puisque $\beta > \alpha$, β n'est pas nul, et puisqu'il est fini, il existe un ordinal δ tel que $\beta = \delta + 1$. On va distinguer deux cas :

- $\delta > \alpha$; par minimalité de β, il existe un ordinal γ' tel $\delta = \alpha + \gamma'$; d'après *i)*, $\beta = \delta + 1 = \alpha + (\gamma' + 1)$: impossible.

- sinon, on voit sans peine que $\delta = \alpha$, et donc $\beta = \alpha + 1$: c'est encore impossible.

☺

REMARQUES : 1) Pour les propriétés *i)-vi)*, on a seulement utilisé le fait que α et β étaient des ensembles ordonnés.

2) Il est facile de voir que la somme et le produit ordinal ne sont pas commutatifs : par exemple $1 + \omega = \omega < \omega + 1$ et $2 \times \omega = \omega < \omega \times 2$. Cet exemple montre aussi qu'il faut faire attention au sens de la distributivité dans *iii)* : on a $2 \times \omega = (1 + 1) \times \omega \neq \omega + \omega$. On peut voir aussi que la propriété *x)* est vraie pour tous les ordinaux.

3) On abandonne à partir de maintenant la notation α^+ pour la remplacer par $\alpha + 1$, comme nous y autorise *vii)*.

Les entiers

2.11 On en sait assez maintenant pour construire les nombres entiers. Considérons l'ensemble ω, et définissons : l'application S de ω dans ω (appelée **fonction successeur**) qui à $n \in \omega$ fait correspondre $n + 1$) ; l'application $+$ de $\omega \times \omega$ dans ω (appelée **addition**) qui à (n,p) fait correspondre $n + p$; enfin l'application $\times$ de $\omega \times \omega$ dans ω (appelée **multiplication**) qui à (n,p) fait correspondre $n \times p$. La structure ainsi définie jouit des propriétés suivantes :

a) l'élément **0** est un élément neutre pour l'addition (théorème 2.10, *iv)*), et 1 est un élément neutre pour la multiplication (théorème 2.10, *vi)*) ;

b) si $n \in \omega$ et si n n'est pas égal à 0, alors il existe un unique élément p de ω tel que $n = S(p)$: cela découle immédiatement de la définition des ordinaux finis et du théorème 2.10, *ix)* ;

c) il n'existe pas d'élément $p \in \omega$ tel que $0 = S(p)$ (découle immédiatement des définitions);

d) l'addition et la multiplication sont associatives (théorème 2.10, *i)* et *ii)*) ;

e) l'addition est distributive par rapport à la multiplication (théorème 2.10, *iii)*) ;

f) D'après *x)* du théorème 2.10, on voit que pour tous n, p appartenant à ω, $n < p$ si et seulement si il existe un ordinal fini non vide q tel que $n + q = p$.

On notera $\mathbb{N}$ la structure $< \omega, 0, S, +, \times >$ et les éléments de ω seront appelés des entiers. Cette dénomination est justifiée par les propriétés a)-f) et le fait que tout

ensemble non vide d'ordinaux (a fortiori d'entiers) admet un élément minimum : on n'utilise pas autre chose pour montrer tous les théorèmes d'arithmétique. Par exemple, le lecteur pourra montrer que l'addition et la multiplication sont des opérations commutatives ; il pourra s'inspirer de la preuve se trouvant au chapitre 6.

A partir de maintenant, le mot « entier » signifiera donc « élément de ω». On a déjà convenu d'écrire $\mathbf{0}$ au lieu de $\emptyset$, $\mathbf{1}$ au lieu de $\{\emptyset\}$, et cette convention est justifiée par le théorème 2.10. Il faudra bien distinguer les entiers, (les éléments de ω) de ce que nous appelons les entiers intuitifs, dont nous nous sommes déjà servis plusieurs fois. En règle générale, c'est quand on parlera du langage (par exemple pour la longueur d'une formule ou le nombre de ses variables libres) que l'on aura besoin de ces entiers intuitifs.

On peut aussi remarquer que, si on se place dans un méta-univers, on peut associer à tout entier intuitif un élément de ω en itérant la construction $\mathbf{0} = \emptyset$, $\mathbf{1} = \{\mathbf{0}\}$, $\mathbf{2} = \{\mathbf{1}\}$, etc. Mais il peut très bien y avoir d'autres éléments dans ω (des entiers « non standard »).

On peut continuer et définir dans $\mathfrak{U}$ toutes les structures mathématiques habituelles : l'anneau des entiers relatifs $\mathbb{Z}$, puis les rationnels, puis les nombres réels, etc. Pour voir comment procéder, il suffit de se reporter à un ouvrage de mathématiques générales, comme par exemple le « cours de Mathématiques de premier cycle (première année) » de Jacques Dixmier (Gauthiers-Villars (Dunod), 1967). Ce qu'il est important de noter, c'est que les structures que l'on obtient ainsi (la base de ces structures, et aussi les opérations) sont des ensembles, c'est-à-dire des points de $\mathcal{U}$.

Rien ne nous empêche de définir dans $\mathfrak{U}$ les suites finies, les formules du premier ordre, les structures et la satisfaction d'une formule dans une structure. On peut alors énoncer les axiomes de Peano et s'apercevoir que $\mathbb{N}$ est un modèle de ces axiomes. Mais on n'accomplira ce dernier pas qu'exceptionnellement : en l'absence d'indication contraire, les mots « formule » , « modèle », etc. garderont leur sens intuitif.

3. DEMONSTRATIONS ET DEFINITIONS PAR INDUCTION

L'induction

3.1 Les ordinaux apparaissent comme une généralisation des entiers. Un des faits qui rend cette intuition intéressante est que l'on peut faire sur les ordinaux des démonstrations par induction. On a d'ailleurs employé ce type de preuve plusieurs fois sans le dire. Le principe est le suivant :

Soit $F[v_0]$ une formule de $\mathscr{L}$ à une variable libre et à paramètres dans $\mathscr{U}$; supposons qu'au cours d'une preuve, on veuille montrer que pour tout ordinal α, $F[\alpha]$ est vrai. On se donne un ordinal β et on fait l'hypothèse (hypothèse d'induction) que, pour tout ordinal $\gamma < \beta$, $F[\gamma]$ est vrai. De cette hypothèse, et des autres données que l'on a à sa disposition, on déduit que $F[\beta]$ est vrai. De là, on déduit que, pour tout ordinal α, $F[\alpha]$ est vrai. Cela s'exprime par les formules suivantes :

(∗) $\forall\alpha(\mathrm{On}[\alpha] \Longrightarrow (\forall\beta(\beta \in \alpha \Longrightarrow F[\beta]) \Longrightarrow F[\alpha])) \Longrightarrow \forall\alpha(\mathrm{On}[\alpha] \Longrightarrow F[\alpha])$.

Le principe se justifie de la façon suivante : supposons que

$$\forall\alpha(\mathrm{On}[\alpha] \Longrightarrow (\forall\beta(\beta \in \alpha \Longrightarrow F[\beta]) \Longrightarrow F[\alpha]))$$

soit vrai. S'il y a un ordinal α pour lequel $F[\alpha]$ est faux, alors il y en a un plus petit (voir 2.6), que nous appellerons α_0. Précisément parce que c'est le plus petit, pour tout ordinal β, $(\beta \in \alpha_0 \Longrightarrow F[\beta])$ est vrai, et donc, par hypothèse, $F[\alpha_0]$ est aussi vrai, ce qui est contradictoire.

Pour montrer (∗), il faut montrer $F[\alpha]$ en supposant que $F[\beta]$ est vrai pour tout $\beta \in \alpha$. Il arrive souvent que cette preuve se scinde en trois cas, suivant que α est égal à 0, qu'il est successeur ou qu'il est limite. Le fait qu'il faille aussi considérer le cas où α est limite constitue une nouveauté par rapport aux démonstrations par récurrence sur les entiers.

3.2 Passons maintenant aux définitions par induction, et pour expliquer ce que l'on va faire, reprenons l'exemple des définitions des fonctions des entiers dans les entiers par récurrence : pour définir une fonction f par récurrence, il faut définir $f(0)$ et se donner les moyens de calculer $f(n+1)$ à partir de $f(n)$. Si on essaye de généraliser ce type de définition aux ordinaux, on voit qu'on aura un problème aux ordinaux limites : comment, par exemple, définir $f(\omega)$? On a vu, par exemple dans l'exercice 13 du chapitre 5, que, dans les définitions par récurrence, on peut se permettre d'utiliser toutes les valeurs $f(i)$, pour $0 \leqslant i \leqslant n$ déjà calculées. C'est plutôt de ces récurrences que l'on va

s'inspirer : pour définir une fonction φ sur les ordinaux, il suffit de savoir définir, pour tout ordinal α, $\varphi(\alpha)$ à partir des valeurs $\varphi(\beta)$ pour $\beta \in \alpha$, c'est-à-dire à partir de l'application de domaine α qui à $\beta \in \alpha$ fait correspondre $\varphi(\beta)$.

La fonction φ que l'on cherche à définir n'est pas une application, puisque son domaine est la classe des ordinaux qui n'est pas un ensemble (voir les remarques qui font suite à la définition 1.9 ; voir aussi la remarque 1 plus loin). Elle sera définie par une formule $G[v_0,v_1]$ telle que :

$$\forall v_0(On[v_0] \Longrightarrow \exists! v_1 G[v_0,v_1])$$

et si α est un ordinal, $\varphi(\alpha)$ sera l'unique ensemble x satisfaisant $G[\alpha,x]$. En revanche, la restriction de cette fonction à un ordinal α est une application : par remplacement, on peut définir un ensemble $A = \{x$; il existe un ordinal $\beta < \alpha$ tel que $G[\beta,x]\}$, et la restriction de φ à α, que l'on notera $\varphi\restriction_\alpha$, est égale à :

$$\{(\beta,x) \in \alpha \times A ; G[\beta,x]\}.$$

Il faut maintenant expliquer ce que l'on entend par « $\varphi(\alpha)$ peut être définie à partir des valeurs $\varphi(\beta)$ pour $\beta < \alpha$ ». Cela veut dire que l'on impose des conditions sur la fonction φ liant $\varphi(\alpha)$ aux valeurs $\varphi(\beta)$ pour $\beta < \alpha$ (exactement comme dans le cas des fonctions récursives), et qui sont suffisamment restrictives pour déterminer complètement $\varphi(\alpha)$ si $\varphi\restriction_\alpha$ est connu. Elles seront exprimées par une formule $F[v_0,v_1,v_2]$ telle que :

(**) $\forall v_0 \forall v_1((On[v_0] \wedge v_1$ est une application de domaine $v_0) \Longrightarrow \exists! v_2 F[v_0,v_1,v_2])$;

On veut alors une fonction φ qui satisfasse :

(*) pour tout ordinal α, $\varphi(\alpha)$ est l'unique ensemble x tel que $F[\alpha,\varphi\restriction_\alpha,x]$.

THEOREME : *Soit* $F[v_0,v_1,v_2]$ *une formule (éventuellement avec paramètres dans* $\mathcal{U}$ *) telle que :*

(**) $\forall v_0 \forall v_1((On[v_0] \wedge v_1$ *est une application de domaine* $v_0) \Longrightarrow \exists! v_2 F[v_0,v_1,v_2])$,

alors, il existe une et une seule fonction φ *dont le domaine est la classe des ordinaux et telle que :*

(*) *pour tout ordinal* α, $\varphi(\alpha)$ *est l'unique ensemble* x *tel que* $F[\alpha,\varphi\restriction_\alpha,x]$.

☺ Considérons la condition suivante portant sur l'application f :

(•) le domaine de f est un ordinal, et pour tout $\beta \in dom(f)$, on a : $F[\beta,f\restriction_\beta,f(\beta)]$.

Il est complètement évident que, si f satisfait (•) et si $\beta \in dom(f)$, alors $f\restriction_\beta$ satisfait aussi (•). On voit aussi que, pour tout ordinal α, il y a au plus une application f de domaine α satisfaisant cette condition ; on raisonne par l'absurde : soient f et f' deux applications différentes de domaine α qui satisfont (•). Soit β le plus petit ordinal tel que

$f(\beta) \neq f'(\beta)$. Alors (minimalité de β), $f \upharpoonright_\beta = f' \upharpoonright_\beta$, et on a : $F[\beta, f \upharpoonright_\beta, f(\beta)]$ et $F[\beta, f \upharpoonright_\beta, f'(\beta)]$; ceci contredit (**).

L'unicité annoncée dans le théorème en découle : si φ et φ' sont des fonctions dont le domaine est la classe des ordinaux et satisfaisant (*), et si α est un ordinal, alors $\varphi \upharpoonright_{(\alpha+1)}$ et $\varphi' \upharpoonright_{(\alpha+1)}$ satisfont (•) et sont donc égales : $\varphi(\alpha) = \varphi'(\alpha)$.

Considérons la formule :

$G[v_0, v_1]$: v_0 est un ordinal et il existe une application f de domaine $v_0 + 1$ satisfaisant (•) et telle que $v_1 = f(v_0)$.

Il est clair, d'après l'unicité que l'on vient de montrer, que cette formule est fonctionnelle en v_0. Appelons φ_G la fonction partielle que cette formule définit.

Supposons un instant que α soit un ordinal et que la fonction φ_G soit définie sur α, c'est-à-dire : pour tout $\beta < \alpha$, il existe un ensemble x tel que $G[\beta, x]$. Par remplacement, l'image de α par φ_G est un ensemble A :

$$A = \{ y \text{ ; il existe un ordinal } \beta \in \alpha \text{ tel que } G[\beta, y] \},$$

et l'ensemble :

$$g = \{ (\beta, y) \in \alpha \times A \text{ , } G[\beta, y] \}$$

est une application de domaine α. Montrons que cette application satisfait (•). Il s'agit de montrer que,

$$\text{pour tout ordinal } \beta, \ \beta < \alpha \text{ implique } F[\beta, g \upharpoonright_\beta, g(\beta)].$$

On raisonne encore par l'absurde, et considérons encore le plus petit ordinal $\beta < \alpha$ tel que $F[\beta, g \upharpoonright_\beta, g(\beta)]$ soit faux. A cause de la minimalité de β, $g \upharpoonright_\beta$ satisfait (•). Puisque $g(\beta)$ satisfait $G[\beta, g(\beta)]$ (par définition de g), on sait qu'il existe une application f de domaine $\beta + 1$ satisfaisant (•) et telle que $f(\beta) = g(\beta)$. On en déduit, d'une part que $f \upharpoonright_\beta = g \upharpoonright_\beta$ (toutes deux satisfont (•)), et d'autre part que $F[\beta, f \upharpoonright_\beta, f(\beta)]$ (f satisfait (•)). Cela montre que $F[\beta, g \upharpoonright_\beta, g(\beta)]$, ce qui est contradictoire.

On peut maintenant montrer par induction que : pour tout ordinal α, il existe une ensemble x satisfaisant $G[\alpha, x]$: supposons que ce soit vrai pour tout $\beta < \alpha$. On vient de voir que $g = \varphi_G \upharpoonright_\alpha$ satisfait (•). Par (**), il existe un ensemble a tel que $F[\alpha, g, a]$. Posons :

$$f = g \cup \{ (\alpha, a) \}$$

Il est alors clair que f est une application de domaine $\alpha + 1$ satisfaisant encore (•), et on a bien $G[\alpha, a]$.

La formule G définit donc une fonction φ_G dont le domaine est la classe des ordinaux, et il découle de ce qu'on a dit que φ_G satisfait (*).

☺

REMARQUE 1 : Il nous arrivera d'avoir besoin de définir par induction une application dont le domaine est un ordinal α fixé (par exemple ω pour les fonctions récursives). Dans

ce cas, la condition (**) est remplacée par la condition plus faible suivante :

$\forall v_0 \forall v_1((v_0$ est un ordinal inférieur à α et v_1 est une application de domaine $v_0) \Longrightarrow \exists! v_2 F[v_0,v_1,v_2])$.

On peut alors montrer qu'il existe une et une seule application f de domaine α telle que, pour tout ordinal $\beta < \alpha$, $f(\beta)$ est l'unique ensemble x tel $F[\beta, f\restriction_\beta, x]$: soit on adapte la démonstration précédente, soit on applique le théorème précédent en utilisant la formule $F'[v_0,v_1,v_2] = (v_0 < \alpha \Longrightarrow F[v_0,v_1,v_2]) \wedge (v_0 \geqslant \alpha \Longrightarrow v_2 \simeq \emptyset)$

REMARQUE 2 : Dans un grand nombre de cas d'applications du théorème ci-dessus, la situation est en fait plus compliquée : reprenons les notations de la démonstration. Tout en définissant par induction $\varphi(\alpha)$, on démontre par induction que l'application $\varphi\restriction_\alpha$ satisfait une certaine formule, disons $P[v_0]$. Le point délicat, c'est que $\varphi(\alpha)$ ne peut être défini que si $\varphi\restriction_\alpha$ satisfait P ; autrement dit, on n'est plus assuré que la condition (**) est vérifiée, mais seulement que :

$\forall v_0 \forall v_1((On[v_0] \wedge v_1$ est une application de domaine $v_0 \wedge P[v_1]) \Longrightarrow \exists! v_2 F[v_0,v_1,v_2])$.

Ici encore, on se ramène au théorème précédent par une pirouette : on remplace la formule F par $F' = (P[v_1] \Longrightarrow F[v_0,v_1,v_2]) \wedge (\neg P[v_1] \Longrightarrow v_2 \simeq \emptyset)$.

L'axiome du choix

3.3 Rappelons d'abord l'énoncé de cet axiome :

(AC) Si $(a_i)_{i \in I}$ est une famille d'ensembles non vides, alors $\prod_{i \in I} a_i$ n'est pas vide.

L'axiome du choix est équivalent, moyennant les axiomes de ZF, à d'autres énoncés plus faciles à exploiter, que nous allons présenter maintenant.

DEFINITION : *On dit qu'un ensemble ordonné* (X,R) *est* ***inductif*** *si, pour tout sous-ensemble* Y *de* X, *si* Y *est totalement ordonné par* R, *alors* Y *admet un majorant dans* X.

Il découle de cette définition que, si (X,R) est inductif, alors X n'est pas vide : l'ensemble vide, qui est un sous-ensemble de X totalement ordonné par R, doit avoir un majorant, et cela fournit un élément de X. Dans la pratique, lorsqu'on veut montrer que

(X,R) est inductif, il est en général plus clair de montrer que X n'est pas vide et que tout sous-ensemble Y non vide de X totalement ordonné par R admet un majorant dans X.

THEOREME : *Les trois énoncés suivants sont équivalents :*

(i) (AC)

(ii) si (X,R) *est un ensemble ordonné inductif, alors il admet au moins un élément maximal.*

(iii) pour tout ensemble X, *il existe un bon ordre sur* X.

Les propriétés *(ii)* et *(iii)* sont donc des théorèmes de ZFC ; *(ii)* est généralement appelé le **théorème** (ou lemme) **de Zorn** et *(iii)* le **théorème de Zermelo**.

☺ *(i)* implique *(ii)* : on raisonne par l'absurde, et on suppose donc, d'une part l'axiome du choix, d'autre part qu'il existe un ensemble inductif (X,R) n'admettant pas d'élément maximal. Considérons :

$$T = \{ Y \in \mathfrak{P}(X) \text{ ; } Y \text{ est totalement ordonné par } R \}.$$

Pour chaque élément Y de T, il existe un élément a dans X qui majore Y ; comme a n'est pas maximal dans X, il existe b dans X tel que $a <_R b$. Donc, pour tout $Y \in T$, l'ensemble

$$\{ b \in X \text{ ; pour tout } y \in Y, y <_R b \}$$

n'est pas vide. D'après l'axiome du choix, il existe donc une application k de T dans X telle que :

$$\text{pour tout } Y \in T, \text{ pour tout } y \in Y, y <_R k(Y).$$

On peut maintenant définir par induction sur la classe des ordinaux une fonction f à valeurs dans X de sorte que : si α et β sont des ordinaux et $\alpha \in \beta$, alors $f(\alpha) < f(\beta)$. Comme c'est la première fois que l'on utilise ce principe d'induction, on va être particulièrement soigneux. Soit $F[v_0,v_1,v_3]$ la formule : $On[v_1] \wedge v_3$ est une application de domaine $v_1 \wedge ((Im(v_3) \in T) \Longrightarrow v_0 \simeq k(Im(v_3)) \wedge ((Im(v_3) \notin T) \Longrightarrow v_0 \simeq \emptyset))$.

Cette formule F est fonctionnelle et les conditions requises par le théorème 3.2 sont satisfaites. On en déduit donc une fonction h qui est telle que pour tout ordinal α, $F[h(\alpha),\alpha,h\restriction_\alpha]$. On montre alors par induction que, pour tout ordinal α, la condition $(\bullet)_\alpha$ suivante est satisfaite :

$(\bullet)_\alpha$ $h(\alpha) \in X$ et ($\beta \in \alpha$ implique $h(\beta) <_R h(\alpha)$).

Supposons que $(\bullet)_\beta$ soit vrai pour tout $\beta \in \alpha$. Alors $\{h(\beta) \text{ ; } \beta \in \alpha\}$ est inclus dans X et est totalement ordonné par R, autrement dit $h[\alpha] \in T$, et donc, d'après la définition inductive de h, $h(\alpha) \in X$ et $h(\beta) <_R h(\alpha)$, pour tout $\beta \in \alpha$.

La contradiction est alors facile à obtenir. Considérons la formule $H[v_0,v_1]$:

$$On[v_0] \wedge v_1 \in T \wedge \text{il existe un isomorphisme de } v_0 \text{ sur } v_1.$$

On a vu (proposition 3 de 2.6) qu'un ensemble ordonné ne pouvait pas être isomorphe à

deux ordinaux différents. Donc, la formule H est fonctionnelle en v_1. Par remplacement, l'image de T par la fonction que cette formule définit est un ensemble. Mais on vient de voir que tout ordinal est isomorphe à un élément de T, et donc cette image serait l'ensemble de tous les ordinaux : cela est contradictoire avec la proposition 1 de 2.6.

(ii) implique *(iii)* : la démonstration qui suit est caractéristique de la façon dont on utilise généralement le lemme de Zorn.

Soit X un ensemble, et il faut montrer qu'il existe un bon ordre sur X. Considérons l'ensemble :

$$\mathfrak{a} = \{ (A,R) \in \mathfrak{P}(X) \times \mathfrak{P}(X \times X) \text{ ; R est une relation de bon ordre sur A} \}$$

et la relation binaire $\mathfrak{s}$ sur $\mathfrak{a}$:

$$\mathfrak{s} = \{ ((A_0,R_0),(A_1,R_1)) \in \mathfrak{a} \times \mathfrak{a} \text{ ; } A_0 \subsetneq A_1, A_0 \text{ est un segment initial de } (A_1,R_1) \text{ et } R_0 = R_1 \restriction_{A_0} \}.$$

Il est immédiat de vérifier que $\mathfrak{s}$ est une relation d'ordre sur $\mathfrak{a}$. Montrons que cette relation est inductive. Tout d'abord $\mathfrak{a}$ n'est pas vide, puisqu'il contient $(\emptyset,\emptyset)$. Soit $\mathfrak{b}$ un sous-ensemble non vide de $\mathfrak{a}$ totalement ordonné par $\mathfrak{s}$. Posons :

$C = \{x \in X \text{ ; il existe } (A,R) \in \mathfrak{b} \text{ tel que } x \in A \}$

et $T = \{ (x,y) \in X \times X \text{ ; il existe } (A,R) \in \mathfrak{b} \text{ tel que } (x,y) \in R \}$.

Montrons que T est un bon ordre sur C. On commence par voir que $T \subseteq C \times C$: si $(x,y) \in T$, alors il existe un couple (A,R) appartenant à $\mathfrak{b}$ tel que $(x,y) \in R$. Comme $(A,R) \in \mathfrak{a}$, R est une relation sur A et donc x et y appartiennent à A. De la définition de C, il découle qu'ils appartiennent aussi à C.

Transitivité de T : supposons que (x,y) et (y,z) appartiennent à T. Il s'agit de montrer que (x,z) appartient aussi à T. Il existe (A_0,R_0) et (A_1,R_1) dans $\mathfrak{b}$ tels que $x <_{R_0} y$ et $y <_{R_1} z$. Or $\mathfrak{b}$ est totalement ordonné par $\mathfrak{s}$; supposons par exemple que $((A_0,R_0) <_{\mathfrak{s}} (A_1,R_1))$ (l'autre cas se traite exactement de la même manière). Cela veut dire que $A_0 \subseteq A_1$ et que $R_0 = R_1 \restriction_{A_0}$, et il en découle que $x <_{R_1} y$. Comme R_1 est une relation d'ordre, $x <_{R_1} z$. L'antiréflexivité de T est facile à établir : si $x \in C$, alors pour tout (A,R) dans $\mathfrak{b}$, (x,x) n'appartient pas à R, et donc, (x,x) n'appartient pas à T.

Il reste à montrer que C est bien ordonné par T (on a remarqué que cela implique que C est totalement ordonné par T). Soit D un sous-ensemble non vide de C ; choisissons un point d de D. Il existe $(A,R) \in \mathfrak{b}$ tel que $d \in A$, et donc $A \cap D$ n'est pas vide. Il admet donc un élément minimum pour R, que nous appellerons a. On va voir que a est minimum dans D pour T. Soit en effet x un autre élément de D, et $(B,S) \in \mathfrak{b}$ tel que $x \in B$. On utilise encore le fait que $\mathfrak{b}$ est totalement ordonné par $\mathfrak{s}$. Si $(B,S) <_{\mathfrak{s}} (A,R)$, alors $B \subseteq A$, $x \in A \cap D$, et, par définition de a, $a <_R x$, et donc $a <_T x$. Si $(A,R) <_{\mathfrak{s}} (B,S)$, alors : si $x \in A$, alors $x \in A \cap D$ et $a <_R x$; si $x \notin A$, alors, parce que A est un segment initial de B pour S, $a <_S x$. Dans les deux cas, $a <_T x$.

On a donc bien montré que l'ensemble $\mathfrak{a}$ ordonné par $\mathfrak{s}$ est inductif ; d'après *ii)*, il admet donc un élément maximal. Soit (D,U) cet élément maximal. On va terminer la preuve en montrant que D est égal à X tout entier.

On raisonne par l'absurde : choisissons un point a de $X - D$. On pose $D' = D \cup \{a\}$, et on étend la relation U en une relation U' sur D' en décrétant que a est supérieur à tous les éléments de D ; alors D' est bien ordonné par U' (même preuve que pour le corollaire 2 de proposition 2.3), et D en est un segment initial. Cela montre que $(D',U') >_{\mathfrak{s}} (D,U)$, ce qui contredit la maximalité de (D,U).

(iii) implique *(i)* : soit $(a_i)_{i \in I}$ une famille d'ensembles non vides. Posons :

$$a = \bigcup_{i \in I} a_i.$$

En utilisant *(iii)*, on voit qu'il existe une relation de bon ordre , disons $<$, sur a. Alors :

$$b = \{(i,x) \in I \times a \ ; \ x \text{ est l'élément minimum de } a_i \text{ pour la relation } <\}$$

appartient à $\prod_{i \in I} a_i$.

☺

4. CARDINALITE

Les classes cardinales

4.1 DEFINITION : *Soient* x *et* y *deux ensembles. On dit que* x *est* ***subpotent à*** y *s'il existe une injection de* x *dans* y. *On dit que* x *et* y *sont* ***équipotents*** *s'il existe une bijection de* x *sur* y.

Considérons la formule

$$F[v_0,v_1] = \exists f(f \text{ est une injection de } v_0 \text{ dans } v_1).$$

On ne peut pas parler de la relation définie par F puisque, a priori, la classe des ensembles (x,y) satisfaisant F[x,y] n'est pas un ensemble (a posteriori, ce n'en est d'ailleurs pas un). On peut cependant remarquer que la méta-relation définie par cette formule est réflexive et transitive, c'est-à-dire que les formules :

$$\forall v_0 F[v_0,v_0] \quad \text{et} \quad \forall v_0 \forall v_1 \forall v_2((F[v_0,v_1] \wedge F[v_1,v_2]) \Longrightarrow F[v_0,v_2])$$

sont vérifiées. De même si on considère la formule :

$$G[v_0,v_1] = \exists f(f \text{ est une bijection de } v_0 \text{ dans } v_1),$$

alors la méta-relation définie par G est réflexive, symétrique et transitive. Elle a donc toutes les propriétés des relations d'équivalence (mais ce n'est pas une relation). En particulier, si x est un ensemble, on peut considérer la classe des éléments équipotents à x. On appellera **classe cardinale de** x cette classe, et on la notera card(x) ; si x est un ensemble et λ est un classe cardinale, on dira que x **est de cardinalité** λ pour dire que x appartient à λ. Dans le cas où x n'est pas l'ensemble vide, on peut vérifer que la classe cardinale de x n'est pas un ensemble.

4.2 On a alors l'important théorème de **Cantor-Bernstein** :

THEOREME : *Si* x *est subpotent à* y *et* y *est subpotent à* x, *alors* x *et* y *sont équipotents.*

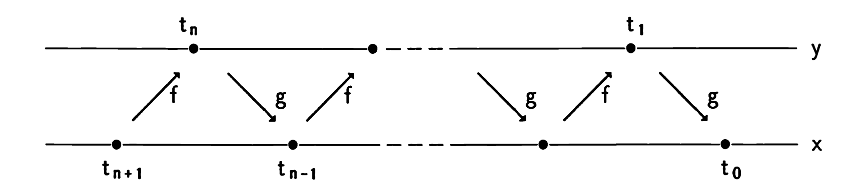
⊖ On considère deux ensembles x et y, une injection f de x dans y et une injection g de y dans x. Il s'agit de construire une bijection h de x sur y.

Puisque f et g sont des injections, chaque élément de x a au plus un antécédent par g dans y, et chaque élément de y a au plus un antécédent par f dans x. Partant d'un élément quelconque $t_0 \in x$, on constitue une « chaîne » t_0, t_1, t_2, ..., dont les éléments sont alternativement dans x et dans y, de telle sorte que chaque élément soit suivi, si possible, de son unique antécédent (par g ou par f, suivant le cas). On voit qu'il y a trois possibilités : ou bien cette chaîne ne s'interrompt jamais, ou bien elle s'interrompt sur un élément de x qui n'a pas d'antécédent par g (c'est le cas en particulier lorsque t_0 lui-même n'appartient pas à l'image de g ; t_1 n'est alors pas défini), ou bien elle s'interrompt sur un élément de y qui n'a pas d'antécédent par f. A ces trois possibilités correspond une partition de l'ensemble x en (au plus) trois sous-ensembles que nous appellerons respectivement x_∞, x_x et x_y.

Si on part d'un élément $u_0 \in y$, on peut définir de manière analogue une chaîne u_0, u_1, u_2, ...telle que, pour tout n, u_{n+1} soit l'unique antécédent de u_n (par f ou par g, suivant la parité de n), lorsqu'un tel antécédent existe, et ne soit pas défini dans le cas contraire. On appelle alors y_∞ l'ensemble des éléments de y qui engendrent une chaîne ininterrompue, y_x l'ensemble de ceux qui engendrent une chaîne qui s'interrompt sur un élément de x qui n'a pas d'antécédent par g, et y_y l'ensemble de ceux qui engendrent une chaîne qui s'interrompt sur un élément de y qui n'a pas d'antécédent par f.

Formellement, il faut d'abord définir, pour tout ensemble a et pour toute application φ de a dans a, par induction sur l'entier $n \in \omega$, l'application φ^n de a dans a : φ^0 est l'identité sur a et, pour tout $k \in \omega$, φ^{k+1} est l'application composée $\varphi \circ \varphi^k$. On pose ensuite :

- $x_x = \{t \in x \text{ ; il existe } k \in \omega \text{ et } u \in x - \text{Im}(g) \text{ tels que } t = (g \circ f)^k(u)\}$;
- $x_y = \{t \in x \text{ ; il existe } k \in \omega \text{ et } v \in y - \text{Im}(f) \text{ tels que } t = g((f \circ g)^k(v))\}$;
- $x_\infty = x - (x_x \cup x_y)$;
- $y_x = \{u \in y \text{ ; il existe } k \in \omega \text{ et } t \in x - \text{Im}(g) \text{ tels que } u = f((g \circ f)^k(t))\}$;
- $y_y = \{u \in y \text{ ; il existe } k \in \omega \text{ et } v \in y - \text{Im}(f) \text{ tels que } u = (f \circ g)^k(v)\}$;
- $y_\infty = y - (y_x \cup y_y)$.



Les faits suivants sont alors clairs : l'image par f de tout élément de x_x appartient à y_x ; l'image par f de tout élément de x_∞ appartient à y_∞ ; tout élément de y_x admet un antécédent par f qui appartient à x_x , tout élément de y_∞ admet un antécédent par f qui appartient à x_∞ ; x_y est inclus dans l'image de g et l'antécédent par g de tout élément de x_y appartient à y_y. Il résulte de ces remarques que la restriction de f à l'ensemble $x_\infty \cup x_x$ est une bijection de $x_\infty \cup x_x$ sur $y_\infty \cup y_x$ (désignons-la par φ), et que la restriction de g à y_y est une bijection de y_y sur x_y (désignons-la par ψ). L'application h de x dans y définie par $h = \varphi \cup \psi^{-1}$ est alors une bijection de x sur y.

On remarquera que les ensembles x_∞, x_x et x_y peuvent éventuellement être vides (en même temps, respectivement, que y_∞, y_x et y_y), mais cela n'affecte en rien la construction précédente.

☺

On remarque que si x, x', y et y' sont des ensembles, si x et x' sont équipotents, si y et y' sont équipotents et si x est subpotent à y, alors x' est subpotent à y' (la composée de deux injections est une injection). Cela permet de définir un ordre sur les classes cardinales : si λ et μ sont deux classes cardinales, on dira que λ est **inférieure ou égale à** μ, et on écrira $\lambda \leqslant \mu$, s'il existe des ensembles x et y, respectivement dans les classes λ et μ, tels que x soit subpotent à y. Si λ, μ et ν sont des classes cardinales, on a :

$\lambda \leqslant \lambda$;

$\lambda \leqslant \mu$ et $\mu \leqslant \lambda$ implique $\lambda = \mu$ (c'est le théorème de Cantor-Bernstein) ;

$\lambda \leqslant \mu$ et $\mu \leqslant \nu$ implique $\lambda \leqslant \nu$.

On peut montrer (voir l'exercice 4) que le fait que cet ordre soit total est équivalent à l'axiome du choix.

Opérations sur les classes cardinales

4.3 On veut maintenant définir un certain nombre d'opérations sur les classes cardinales. Pour cela on a besoin de la proposition suivante :

PROPOSITION : *1°) Si* x *est équipotent à* y *et* z *est équipotent à* t, *alors* $x \cup z$ *est équipotent à* $y \cup t$, $x \times z$ *est équipotent à* $y \times t$ *et* x^z *est équipotent à* y^t.

2°) Soient x, y, z *et* t *des ensembles et on suppose que* x *est subpotent à* y *et que* z *est subpotent à* t. *Alors* $x \cup z$ *est subpotent à* $y \cup t$, $x \times z$ *est subpotent à* $y \times t$. *Si* y *n'est pas vide,* x^z *est subpotent à* y^t.

⊖ Commençons par montrer *2°)* : soient f une injection de x dans y et g une injection de z dans t. On vérifie facilement que l'application k dont la définition suit est une injection de $x \cup z$ dans $y \cup t$: si $a \in x \cup z$, alors, soit il existe $b \in x$ tel que $a = (b,0)$, soit il existe $c \in z$ tel que $a = (c,1)$. Dans le premier cas, on pose $k(a) = (f(b),0)$; dans le second, on pose $k(a) = (g(b),1)$. Cela montre que $x \cup z$ est subpotent à $y \cup t$.

On montre de façon analogue que $x \times z$ est supotent à $y \times t$: il suffit de vérifier, ce qui est facile, que l'application h de $x \times z$ dans $y \times t$ définie par :

pour tout $a \in x$ et pour tout $b \in y$, $h((a,b)) = (f(a),g(b))$

est injective.

Le cas de l'exponentiation est un peu plus délicat. On va, dans un premier temps, supposer que z est équipotent à t et que g est une bijection de z sur t. Rappelons que x^z est l'ensemble des applications de z dans x et que y^t est l'ensemble des applications de t dans y. Si $\alpha \in x^z$, posons $i_\alpha = f \circ \alpha \circ g^{-1}$; i_α est donc une application de t dans y. Montrons que l'application de x^z dans y^t qui à α fait correspondre i_α est injective. Pour cela, on suppose que α et β sont deux éléments distincts de x^z et on montre que i_α est différent de i_β : il existe un élément a de z tel que $\alpha(a) \neq \beta(a)$. Posons $b = g(a)$. Alors $i_\alpha(b) = f(\alpha(a))$ et $i_\beta(b) = f(\beta(a))$. Comme f est injective et comme $\alpha(a) \neq \beta(a)$, on a : $i_\alpha(b) \neq i_\beta(b)$.

Revenons au cas général et supposons seulement que g est une injection. Posons $u = g(z)$. Alors g est une application bijective de z sur u, et on vient donc de voir que x^z est subpotent à y^u. Montrons que y^u est subpotent à y^t : choisissons un élément c de y (y n'est pas vide). Si α est une application de u dans y, on peut définir une application j_α de t dans y par :

si $a \in u$, alors $j_\alpha(a) = \alpha(a)$;
si $a \in t - u$, $j_\alpha(a) = c$.

Il est bien clair que si $j_\alpha = j_\beta$, alors $\alpha = \beta$, et on a bien trouvé une application injective de y^u dans y^t.

On remarque qu'avec nos définitions $0^0 = 1$ tandis que $0^1 = 0$: l'hypothèse « y non vide » est donc indispensable.

1°) On peut refaire les preuves précédentes et s'apercevoir que, si les applications f et g sont bijectives, alors les différentes applications de $x \dot\cup z$ dans $y \dot\cup t$, de $x \times z$ dans $y \times t$, de x^z dans y^t qui y sont définies sont alors bijectives. Les paresseux pourront aussi déduire de la première partie que $x \dot\cup z$ est subpotent à $y \dot\cup t$ et que $y \dot\cup t$ est subpotent à $x \dot\cup z$ et appliquer le théorème de Cantor-Berstein (et faire le même raisonnement pour le produit et l'exponentiation). Pour l'exponentiation, il faut, de toutes façons, traiter à part le cas où y est vide, qui est évident.

☺

La définition suivante est donc justifiée :

DEFINITION : *Soient λ et μ deux classes cardinales ; alors $\lambda + \mu$, $\lambda \times \mu$ et λ^μ sont respectivement les classes cardinales de $x \dot\cup y$, $x \times y$ et x^y, où x est un ensemble de cardinalité λ et y est un ensemble de cardinalité μ.*

Voici une petite remarque destinée à nous simplifier la vie ultérieurement :

REMARQUE : Soient x et y deux ensembles. On peut définir une injection f de $x \cup y$ dans $x \dot\cup y$: soit $a \in x \cup y$; si $a \in x$, $f(a) = (a,0)$; sinon, $a \in y$ et on pose, $f(a) = (a,1)$. Ceci montre que :

$$\text{card}(x \cup y) \leqslant \text{card}(x) + \text{card}(y)$$

Si x et y sont disjoints, alors f est une bijection de $x \cup y$ sur $x \dot\cup y$ et

$$\text{card}(x \cup y) = \text{card}(x) + \text{card}(y).$$

Le lecteur pourra s'amuser à montrer, que, dans le cas général :

$$\text{card}(x \cup y) + \text{card}(x \cap y) = \text{card}(x) + \text{card}(y).$$

La proposition 4.3 montre aussi :

COROLLAIRE : *Soient λ, μ, ν, κ des classes cardinales, et supposons que $\lambda \leqslant \mu$ et que $\nu \leqslant \kappa$. Alors $\lambda + \nu \leqslant \mu + \kappa$, $\lambda \times \nu \leqslant \mu \times \kappa$ et, si μ n'est pas égal à 0, $\lambda^\nu \leqslant \mu^\kappa$.*

Attention : ceci devient faux si on remplace les inégalités larges par des inégalités strictes (voir 4.14 et exercice 14).

4.4 PROPOSITION : *Soient λ, μ et ν des classes cardinales. Alors :*

1) $\lambda + (\mu + \nu) = (\lambda + \mu) + \nu$;
2) $\lambda + \mu = \mu + \lambda$;
3) $\lambda \times (\mu \times \nu) = (\lambda \times \mu) \times \nu$;
4) $\lambda \times \mu = \mu \times \lambda$;
5) $\lambda \times (\mu + \nu) = (\lambda \times \mu) + (\lambda \times \nu)$;
6) $\lambda^{\nu} \times \mu^{\nu} = (\lambda \times \mu)^{\nu}$;
7) $\lambda^{\mu+\nu} = \lambda^{\mu} \times \lambda^{\nu}$;
8) $(\lambda^{\mu})^{\nu} = \lambda^{\mu \times \nu}$.

⊖ Soient x, y et z des ensembles de cardinalités respectives λ, μ et ν, et on va supposer que ces ensembles sont deux à deux isjoints.

1) On a vu (en 1.5) que $x \cup (y \cup z) = (x \cup y) \cup z$. Or la cardinalité du premier de ces ensembles est $\lambda + (\mu + \nu)$ et celle du second $(\lambda + \mu) + \nu$ (d'après la remarque 4.3, puisque les ensembles x, y et z sont deux à deux disjoints).

2) De même, $x \cup y$, dont la cardinalité est $\lambda + \mu$, est égal à $y \cup x$ dont la cardinalité est $\mu + \lambda$.

3) L'application f définie par : pour tout $a \in x$, pour tout $b \in y$, pour tout $c \in z$, $f((a,(b,c))) = ((a,b),c)$ est une bijection de $x \times (y \times z)$ sur $(x \times y)$ z.

4) L'application f définie par : pour tout $a \in x$, pour tout $b \in y$, $f((a,b)) = (b,a)$ est une bijection de $x \times y$ sur $y \times x$.

5) On vérifie d'abord que $x \times y$ et $x \times z$ sont des ensembles disjoints ; ensuite que l'ensemble $x \times (y \cup z)$ (dont la cardinalité est $\lambda \times (\mu + \nu)$) est égal à l'ensemble $(x \times y) \cup (x \times z)$ (dont la cardinalité est $(\lambda \times \mu) + (\lambda \times \nu)$).

6) Soient α une application de z dans x et β une application de z dans y. Définissons une application $i_{\alpha,\beta}$ de z dans $x \times y$: pour tout $c \in z$, $i_{\alpha,\beta}(c) = (\alpha(c),\beta(c))$. On vérifie facilement que l'application f qui, à (α,β), fait correspondre $i_{\alpha,\beta}$, est une bijection de $x^z \times y^z$ sur $(x \times y)^z$.

7) Soit α une application de y dans x et β une application de z dans x. Puisque y et z sont disjoints, $\alpha \cup \beta$ est une application de $y \cup z$ dans x, et on voit sans peine que l'application qui à (α,β) fait correspondre $\alpha \cup \beta$ est une bijection de $x^y \times x^z$ sur $x^{y \cup z}$.

8) Soient α une application de $y \times z$ dans x. Pour tout élément c de z, on peut définir une application α_c de y dans x par : pour tout $b \in y$, $\alpha_c(b) = \alpha(b,c)$; cela permet

de définir une application i_α de z dans x^y par : pour tout $c \in z$, $i_\alpha(c) = \alpha_c$. Enfin, on vérifie que l'application qui à α fait correspondre i_α est une bijection de $x^{y \times z}$ sur $(x^y)^z$.
☺

4.5 Avant d'aller plus loin, remarquons que, pour tout ensemble x, $\mathfrak{P}(x)$ est équipotent à $\mathbf{2}^x$. Définissons d'abord la notion de fonction caractéristique d'un sous-ensemble de x : si y est un sous-ensemble de x, alors **la fonction caractéristique** χ_y de y est l'application de x dans $\mathbf{2}$ définie par : pour tout $a \in x$, $\chi(a) = \mathbf{1}$ si $a \in y$ et $\chi(a) = \mathbf{0}$ sinon. L'application qui à y fait correspondre χ_y est une bijection de $\mathfrak{P}(x)$ sur $\mathbf{2}^x$.

Le théorème suivant, appelé **théorème de Cantor**, est important car il montre qu'il n'y a pas de cardinalité maximale :

THEOREME : *Pour toute classe cardinale λ, on a : $\mathbf{2}^\lambda > \lambda$.*

☹ Soit x un ensemble de cardinalité λ. On peut facilement définir une injection f de x dans $\mathfrak{P}(x)$ par : pour tout $a \in x$, $f(a) = \{a\}$. Cela montre que $\lambda \leqslant \mathbf{2}^\lambda$. On va utiliser un argument diagonal pour prouver qu'il n'existe pas de surjection de x sur $\mathfrak{P}(x)$: soit δ une application de x dans $\mathfrak{P}(x)$. Considérons :

$$y = \{a \in x \,;\, a \notin \delta(a)\}.$$

Alors y est un élément de $\mathfrak{P}(x)$ et on va montrer que δ n'est pas surjective en montrant que y n'appartient pas à l'image de δ : raisonnons par l'absurde et supposons que $y = \delta(b)$, où $b \in x$. Si $b \in y$, alors, par définition de y, $b \notin \delta(b)$, ce qui n'est pas possible puisque $\delta(b) = y$. D'un autre côté, si $b \notin y$, alors, toujours par définition de y, $b \in \delta(b) = y$, ce qui est tout aussi impossible.
☺

Les cardinaux finis

4.6 DEFINITION : *On dit qu'un **ensemble est fini** s'il est équipotent à un entier. Un **ensemble infini** est un ensemble qui n'est pas fini.*

Rappelons qu'un entier n est égal à l'ensemble des entiers qui lui sont inférieurs. On a déjà une notion d'ordinal fini (2.7). Avant toute chose, il faut vérifier que les deux définitions concordent. Il est bien évident qu'un ordinal fini (c'est-à-dire un entier) est

en bijection avec lui-même, et est donc fini au sens de la définition ci-dessus. La réciproque (un ordinal infini au sens de 2.7 n'est pas un ensemble fini) va découler du corollaire 1 ci-dessous.

THEOREME : *Soient* n *un entier et* f *une application de* n *dans* n. *Alors :*

1°) si f *est injective, alors* f *est bijective ;*

2°) si f *est surjective, alors* f *est bijective.*

☹ 1°) Par récurrence sur n : c'est clair si $n = 0$, puisque dans ce cas, la seule application de n dans n est surjective. On suppose donc le résultat vrai pour n, et on va le montrer pour n + 1 : soit f une injection de n + 1 dans n + 1. Considérons la bijection h de n + 1 sur n + 1 définie par :

- $h(p) = p$ si $p \neq n$ et si $p \neq f(n)$;
- $h(n) = f(n)$;
- $h(f(n)) = n$.

(Cette définition est cohérente même si f(n) est égal à n). Alors $g = h \circ f$ est aussi une injection de n + 1 dans n + 1 ; de plus, $g(n) = n$, et par conséquent, $g \restriction_n$ est une injection de n dans n. Par hypothèse de récurrence, $g \restriction_n$ est une bijection de n sur n. Donc, tout entier inférieur à n est dans l'image de g, de même que n ($g(n) = n$). On voit donc que g est une bijection de n + 1 sur n + 1, de même que f, qui est égale à $h^{-1} \circ g$.

2°) Soit f une application surjective de n sur n. Considérons l'application h définie par : pour tout $p \in n$, h(p) est le plus petit entier k tel que $f(k) = p$. Alors $f \circ h$ est égale à l'application identique sur n, ce qui implique que h est injective. Donc, d'après 1°), h est une bijection de n sur n, de même que f qui est égale à h^{-1}.

☺

COROLLAIRE 1 : *Soient* α *un ordinal,* n *un entier et supposons* $\alpha > n$ *; alors il n'existe pas d'application injective de* α *dans* n.

☹ On raisonne par l'absurde : soit f une application injective de α sur n : $f \restriction_n$ est aussi injective, donc d'après le théorème, elle est surjective sur n, et si β appartient à α mais pas à n (un tel élément existe puisque $\alpha > n$), $f(\beta)$ appartient à l'image de n par f, ce qui contredit l'injectivité de f.

☺

REMARQUE : On verra en 4.11 une généralisation de l'argument utilisé pour 2°).

COROLLAIRE 2 : *Si* x *est un ensemble fini, alors toute application injective (ou surjective) de* x *dans* x *est bijective.*

☹ Comme x est fini, il existe un ordinal fini α et une bijection f de x sur α. Soit h une application injective de x dans x. Alors $k = fohof^{-1}$ est une application injective de α dans α, et par le théorème 4.6, c'est une bijection. Il est en de même de h qui est égal à $f^{-1}okof$. Le cas où h est une application surjective se traite de la même façon.
☺

4.7 PROPOSITION 1 : *Si* x *est fini, il existe un et un seul entier* n *équipotent à* x.

☹ Par définition, il existe un tel entier. Si x est équipotent à deux entiers n et m, alors n et m sont eux-même équipotents, et le corollaire 1 de 4.6 montre qu'il est impossible que l'on ait $n > m$ ou $m > n$. Il faut donc que n et m soient égaux.
☺

PROPOSITION 2 : *Si* x *est fini et si* y *est subpotent à* x, *alors* y *est fini.*

☹ Soient g une application injective de y dans x et f une bijection de x sur un entier n. Appelons z l'image de y par fog. Alors $fog\restriction y$ est une bijection de y sur z, et il suffit donc de montrer que z est fini. L'ensemble z, muni de la relation d'ordre induite par celle de n (n est un ordinal) est bien ordonné, donc isomorphe à un ordinal α (proposition 3 de 2.6) qui est nécessairement inférieur ou égal à n (lemme 2.6), donc fini.
☺

PROPOSITION 3 : *S'il existe une application* f *surjective d'un ensemble fini* x *sur un ensemble* y, *alors* y *est fini.*

☹ Il existe un entier n et une bijection h de n sur x ; alors foh est surjective de n sur y. On définit une application injective k de y sur x par : pour tout $a \in y$, $k(a)$ est le plus petit entier $m < n$ tel que $foh(m) = a$. On applique alors la proposition 2.
☺

PROPOSITION 4 :

1°) l'union de deux ensembles finis est un ensemble fini ;

2°) le produit de deux ensembles finis est un ensemble fini ;

3°) l'union et le produit d'une famille finie d'ensembles finis sont des ensembles finis.

4°) si a *et* b *sont des ensembles finis, alors* a^b *est un ensemble fini ;*

5°) si A *est un ensemble fini d'ordinaux finis (c'est-à-dire d'entiers), alors* sup A *est un ordinal fini (c'est-à-dire un entier).*

☹ Soient a et b des ensembles finis respectivement équipotents aux entiers n et m.

1°) On a vu (remarque 4.3) que $\text{card}(a \cup b) \leqslant \text{card}(a \,\dot\cup\, b)$ et (proposition 4.3) que $\text{card}(a \,\dot\cup\, b) = \text{card}(n) + \text{card}(m) = \text{card}(n \,\dot\cup\, m)$. Or, d'après le théorème 2.10, *ix)*, $n \,\dot\cup\, m$ est équipotent à un entier ; on conclut avec la proposition 2.

2°) Le cas du produit est encore plus simple : $\text{card}(a \times b) = \text{card}(n \times m)$ (proposition 4.3), et $n \times m$ est fini, par le théoréme 2.10, *ix)*.

3°) Soient I un ensemble fini de cardinalité p, et, pour chaque $i \in I$, a_i un ensemble de cardinalité n_i. On montre par récurrence sur p que $\bigcup_{i \in I} a_i$ et $\prod_{i \in I} a_i$ sont des ensembles finis. C'est évident si $p = 0$. Si $p \neq 0$, soit j un élément de I ; posons $J = I - \{j\}$. La cardinalité de J est égale à $p - 1$, donc par hypothèse de récurrence, $\bigcup_{i \in J} a_i$ et $\prod_{i \in J} a_i$ sont finis, et on conclut avec *1°)* et *2°)* en remarquant que :

$$\bigcup_{i \in I} a_i = \bigcup_{i \in J} a_i \cup a_j \text{ et } \text{card}(\prod_{i \in I} a_i) = \text{card}(\prod_{i \in J} a_i) \times \text{card}(a_j).$$

4°) En se reportant aux définitions 1.9, on voit que $a^b = \prod_{x \in b} a$; *4°)* se déduit donc immédiatement de de *3°)*

5°) se déduit de *1°)* et de *2°)*.

☺

Si λ est la classe cardinale d'un ensemble fini, il y a dans λ un représentant canonique, qui est l'unique entier n figurant dans λ. On fera l'abus de langage consistant à confondre n et card(n). Il y a quelques inconvénients à faire cela (par exemple, $n \times m$ désigne-t-il le produit d'ensembles ou bien le produit de cardinaux ?), mais le contexte sera, en principe, suffisamment clair.

Le dénombrable

4.8 DEFINITION : *On dit qu'un* ***ensemble est dénombrable*** *s'il est équipotent à* ω.

On notera $\aleph_0$ (lire « aleph zéro » ; aleph est la première lettre de l'alphabet hébraïque) la classe cardinale de ω (donc de tout ensemble dénombrable). On voit donc que $\aleph_0$ est strictement supérieur à tous les cardinaux finis. Remarquons que si α est un ordinal, alors sa cardinalité est soit finie, soit supérieure ou égale à $\aleph_0$. Cette propriété s'étend bien sûr à tout ensemble bien ordonné.

PROPOSITION : *Si* x *est dénombrable et* y *est subpotent à* x, *alors* y *est dénombrable ou fini.*

☹ On s'inspire de la preuve de la proposition 2 de 4.7 : y est équipotent à un sous-ensemble z de ω ; parce qu'il est naturellement bien ordonné, z est lui-même équipotent à un ordinal α, qui (remarque 2.6) est inférieur ou égal à ω ; si α est un entier, alors y est fini. Sinon, il est égal à ω et y est dénombrable.
☺

REMARQUE : L'analogue du corollaire 1 de 4.6 est faux pour le dénombrable : l'application f de ω dans ω définie par : $f(n) = n + 1$ est injective, mais non bijective, puisque 0 n'appartient pas à son image. On peut d'ailleurs définir une application injective non surjective de n'importe quel ordinal infini dans lui-même : il suffit de prolonger f par : $f(\beta) = \beta$ pour tout $\beta \geqslant \omega$. En fait, il y a bien pire :

4.9 THEOREME : *1°) L'union de deux ensembles finis ou dénombrables est fini ou dénombrable.*

2°) Le produit de deux ensembles finis ou dénombrables est fini ou dénombrable.

3°) Soit X *un ensemble fini ou dénombrable ; alors l'ensemble* $S = \bigcup_{n \in \omega} X^n$ *est fini ou dénombrable.*

Remarquez que *3°)* affirme que l'ensemble des suites finies d'un ensemble fini ou dénombrable est fini ou dénombrable.

☹ 1°) Soient X et Y deux ensembles finis ou dénombrables. Il existe donc des injections f et g de X et Y, respectivement, dans ω. Pour montrer que $X \cup Y$ est fini ou dénombrable, on va construire une injection h de $X \cup Y$ dans ω. La voici : soit $x \in X \cup Y$; si $x \in X$, on pose $h(x) = 2f(x)$; sinon, $x \in Y$, et on pose $h(x) = 2g(x) + 1$.

2°) Soient encore X et Y deux ensembles finis ou dénombrables et f et g des injections de X et Y, respectivement, dans ω. Voici une injection h de $X \times Y$ dans ω : si $(x,y) \in X \times Y$, alors $h((x,y)) = \alpha_2(f(x),g(y))$, où α_2 est la bijection définie au chapitre 5, 1.11.

3°) Soient X un ensemble fini ou dénombrable et f une injection de X dans ω. On définit une application h de S dans $\bigcup_{n \in \omega} \omega^n$: soit a un élément de S ; il existe donc un entier n tel que a soit une application de n dans X. On pose alors $h(a) = f \circ a$ (intuitivement, si $a = (x_1,x_2,\ldots,x_n)$, alors $h(a) = (f(x_1),f(x_2),\ldots,f(x_n))$). On vérifie sans peine que h est une injection de S dans $\bigcup_{n \in \omega} \omega^n$. D'autre part, l'application Ω définie en 1.12 du chapitre 5 est un injection de $\bigcup_{n \in \omega} \omega^n$ dans ω ; $\Omega \circ h$ est un injection de S dans ω.
☺

REMARQUE : La démonstration qui vient d'être faite utilise quelques faits élémentaires d'arithmétique. Mais ces faits se démontrent sans peine avec tout ce que l'on sait sur $\mathbb{N}$.

La proposition 3 de 4.7 se généralise, avec la même preuve :

PROPOSITION : *S'il existe une application surjective d'un ensemble dénombrable* x *sur* y, *alors* y *est dénombrable ou fini.*

COROLLAIRE : *On a :*

1°) $\aleph_0 + \aleph_0 = \aleph_0$;

2°) $\aleph_0 \times \aleph_0 = \aleph_0$;

3°) pour tout entier n *non nul,* $\aleph_0^n = \aleph_0$;

☹ On vient de voir que $\aleph_0 + \aleph_0$, $\aleph_0 \times \aleph_0$ et $\aleph_0^n$ sont au plus dénombrables. Il suffit de voir que ce ne sont pas des cardinalités finies, ce qui est à peu près évident.
☺

4.10 Pour donner un exemple d'application de la notion de cardinalité, on va montrer qu'il existe des nombres réels qui ne sont pas algébriques. Il existe, par ailleurs, des preuves purement algébriques de ce fait, mais la démonstration qui suit montrera que « la plupart » des réels ne sont pas algébriques (avec comme conséquence, par exemple, que l'ensemble des réels algébriques est de mesure de Lebesgue 0). Rappelons qu'un nombre est **algébrique** s'il est racine d'un polynôme non nul à coefficients dans $\mathbb{Z}$. La stratégie de la démonstration qui suit est simple : on montre, premièrement que la cardinalité de $\mathbb{R}$, l'ensemble des nombres réels est $2^{\aleph_0}$, deuxièmement que l'ensemble des nombres algébriques est dénombrable.

PROPOSITION 1 : $\mathrm{card}(\mathbb{R}) = 2^{\aleph_0}$.

☹ On considère la fonction α de 2^ω dans $\mathbb{R}$ définie comme suit : si $h \in 2^\omega$, alors

$$\alpha(h) = \Sigma_{n=0}^{\infty} \frac{h(n)}{2^{n+1}}$$

(Autrement dit, $0{,}h(0)h(1)\ldots h(n)\ldots$ est le développement de $\alpha(h)$ en écriture binaire). L'image de α est l'intervalle $[0,1]$, mais α n'est pas injective : par exemple, $0{,}1000\ldots$ et $0{,}0111\ldots$ représentent le même réel. Cependant, ce phénomène est très limité. Disons qu'un élément h de 2^ω est **nul à l'infini** s'il existe un entier n tel que $h(p) = 0$ pour tout $p > n$, et posons :

$$S = \{ h \in 2^\omega \,;\, h \text{ n'est pas nul à l'infini} \}.$$

On supposera connu le fait que $\alpha\restriction_S$ est une application bijective de S sur $]0,1]$. Définissons une nouvelle application β de 2^ω dans $\mathbb{R}$ par : si $h \in S$, alors $\beta(h) = 1 + \alpha(h)$; sinon, $\beta(h) = \alpha(h)$. On voit sans trop de difficulté que β est injective, ce qui montre que $\mathrm{card}(\mathbb{R}) \geqslant 2^{\aleph_0}$. D'autre part, l'application f définie par :

$$f(x) = \frac{1}{\pi}\,\mathrm{Arctg}(x) + \frac{1}{2},$$

est une application bijective de $\mathbb{R}$ sur $]0,1[$; on a donc

$$\mathrm{card}(\mathbb{R}) = \mathrm{card}(]0,1[) \leqslant \mathrm{card}(]0,1]) = \mathrm{card}(S) \leqslant 2^{\aleph_0}.$$

Avec le théorème de Cantor Bernstein, on en déduit : $\mathrm{card}(\mathbb{R}) = 2^{\aleph_0}$.

☺

On dit quelquefois que $\mathbb{R}$ a **la puissance du continu** pour dire que $\mathrm{card}(\mathbb{R}) = 2^{\aleph_0}$.

PROPOSITION 2 : *L'ensemble* A *des nombres algébriques réels est dénombrable.*

☹ L'ensemble $\mathbb{Z}$ est la réunion de deux ensembles dénombrables (les entiers positifs et les entiers négatifs), et est donc dénombrable. L'ensemble S des suites finies d'éléments de $\mathbb{Z}$ est aussi dénombrable (théorème 4.9, *3°*)). Pour tout $s=(a_0,a_1,\ldots,a_n)\in S$, posons :

$Z(s)=\emptyset$ si tous les a_i, pour i compris entre 0 et n, sont nuls ;

$Z(s)=\{x\in\mathbb{R} ; a_0+a_1x+\ldots+a_nx^n=0\}$ sinon.

Il existe une application surjective de S sur l'ensemble $\{Z(s) ; s\in S\}$, qui est donc dénombrable (proposition 4.9) ; chaque ensemble $Z(s)$, pour $s\in S$, est fini. De plus, A est la réunion de la famille $(Z(s) ; s\in S)$. Soit f une bijection de ω sur S. On définit une application g de $\omega\times\omega$ dans A par :

• si $Z(f(n))$ a au moins p éléments, alors $g(n,p)$ est le p-ème élément de $Z(f(n))$ (muni de l'ordre induit par celui de $\mathbb{R}$) ;

• sinon, $g(p,n)=0$.

On voit alors que g est surjectif. Comme $\omega\times\omega$ est dénombrable il découle de la proposition 4.9 que A est dénombrable.

☺

L'exercice 23 montre aussi que $\mathbb{R}$ n'est pas dénombrable en utilisant directement un argument diagonal.

Les cardinaux

4.11 A partir de maintenant, certains théorèmes vont nécessiter l'axiome de choix. On signalera ce fait par le sigle (AC).

DEFINITION : *On appelle* ***cardinal*** *un ordinal qui n'est équipotent à aucun ordinal strictement plus petit. (on dit quelquefois* ***ordinal initial****.)*

Par exemple, les ordinaux finis sont des cardinaux (4.6, corollaire 1) ; ω est aussi un cardinal. En revanche, $\omega+1$, $\omega+\omega$, $\omega\times\omega$ ne sont pas des cardinaux (corollaire 4.9). Les cardinaux infinis sont des ordinaux limites : si α est un ordinal infini, l'application f définie comme suit est une bijection de $\alpha+1$ sur α : si $\beta\in\omega$, alors $f(\beta)=\beta+1$; si $\omega\leqslant\beta<\alpha$, alors $f(\beta)=\beta$; $f(\alpha)=0$.

Soit α un ordinal ; il est clair que la classe des ordinaux β tel que α soit subpotent à β n'est pas vide (α en fait partie) et que l'élément minimum de cette classe

est un cardinal. Plus généralement, soit x un ensemble, et supposons qu'il existe un ordinal α tel que x soit subpotent à α. Alors il existe un et un seul cardinal β tel que x soit équipotent à β. L'unicité est évidente puisque deux cardinaux distincts ne peuvent être équipotents. D'autre part, soit β le plus petit ordinal tel que x soit subpotent à β. On voit que cet ordinal est nécessairement un cardinal : on l'appelle **cardinal de** x. Des définitions, il découle que le cardinal d'un ordinal α est un ordinal inférieur ou égal à α.

Si α et β sont des cardinaux, alors $\alpha > \beta$ est équivalent à $\mathrm{card}(\alpha) > \mathrm{card}(\beta)$. Ceci n'est plus vrai en général si α et β sont des ordinaux quelconques (prendre, par exemple, $\alpha = \omega + 1$ et $\beta = \omega$).

A l'aide de la proposition 3 de 2.6, le théorème de Zermelo peut être reformulé de la façon suivante :

THEOREME (AC) : *Pour tout ensemble, il existe un ordinal qui lui est équipotent.*

Supposons, jusqu'à la fin de cette sous-section, que l'axiome du choix est vérifié. Avec la remarque qui précède, on voit que tout ensemble est équipotent à un cardinal, autrement dit que le cardinal de tout ensemble existe. Ceci implique d'ailleurs que la relation $\leqslant$ sur les classes cardinales est totale (voir exercice 4, où la réciproque est aussi démontrée). On voit qu'alors la classe cardinale d'un ensemble x est avantageusement remplacée par le cardinal de cet ensemble, qui en est, en quelque sorte, un représentant canonique. On fera un abus de langage assez courant consistant à ne pas distinguer nettement entre la classe cardinale d'un ensemble X (qui, rappelons-le n'est pas un ensemble) et le cardinal de X (qui est un ordinal). Cela présente évidemment quelques inconvénients (les mêmes que de confondre cardinaux finis et ordinaux finis, voir 4.7, dernier paragraphe). Les ambiguïtés qui pourraient apparaître sont en général levées par le contexte : lorsqu'on fait un calcul de cardinalité, alors c'est la somme cardinale qu'il faut employer ; si c'est un cacul sur les ordinaux (ce qui nous arrivera plus rarement), c'est la somme ordinale. De toute façon, rien n'empêche de préciser s'il y a la moindre possibilité de doute.

Puisqu'on en est aux conséquences de l'axiome du choix, voici une proposition très utile :

PROPOSITION (AC) : *Supposons que* f *soit une application surjective d'un ensemble* a *sur un ensemble* b. *Alors* $\mathrm{card}(b) \leqslant \mathrm{card}(a)$.

☹ En utilisant le théorème de Zermelo, on trouve une relation de bon ordre R sur a. On définit une injection h de b dans a : soit $x \in b$; alors l'ensemble :

$$\{y \in a \, ; \, f(y) = x\}$$

n'est pas vide, puisque f est surjective, et, par définition, h(x) est le plus petit élément (pour R) de cet ensemble.

☺

4.12 La classe des cardinaux n'admet pas d'élément maximum :

THEOREME : *Pour tout cardinal α, il existe un ordinal β tel que* $\mathrm{card}(\beta) > \mathrm{card}(\alpha)$.

☹ Remarquez d'abord qu'avec l'axiome du choix, ce théorème est évident : il suffit de considérer le cardinal de 2^{α} : on sait déjà qu'il est strictement supérieur à α (théorème 4.5).

Sans axiome du choix, la démonstration est un peu plus difficile. On va montrer que la classe des ordinaux subpotents à α est un ensemble. Considérons :

$$R = \{ (X,r) \in \mathfrak{P}(\alpha) \times \mathfrak{P}(\alpha \times \alpha) \, ; \, X \subseteq \alpha \text{ et } r \text{ est un bon ordre sur } X \}.$$

On a vu (proposition 3 de 2.6) que, pour tout $(X,r) \in R$, il existe un et un seul ordinal β tel que $(\beta,\in)$ soit isomorphe à (X,r). Par remplacement, l'image de la fonction qui à $(X,r) \in R$ fait correspondre l'unique ordinal β tel que $(\beta,\in)$ soit isomorphe à (X,r) est un ensemble. Mais c'est précisément la classe des ordinaux subpotents à α : si $(\beta,\in)$ est isomorphe à $(X,r) \in R$, alors il existe bien une bijection de β sur X, qui est une injection de β dans α. Réciproquement, si f est une injection de β dans α, alors, f est une bijection de β sur son image que nous appellerons X, et

$$r = \{ (x,y) \in X \times X \, ; \, f^{-1}(x) \in f^{-1}(y) \}$$

est un bon ordre sur X qui est isomorphe (par f) à $(\beta,\in)$.

Il est clair que l'ensemble $\{\beta \, ; \, \beta$ est un ordinal subpotent à $\alpha\}$ est transitif : c'est donc un ordinal γ (proposition 2.3). On remarque que β n'est pas subpotent à α : sinon il s'appartiendrait à lui-même, ce qui n'est pas possible. C'est donc le plus petit ordinal dont la cardinalité soit strictement supérieure à celle de α : γ est un cardinal strictement supérieur à α.

☺

Si α est un cardinal, on appellera **cardinal successeur de α** et on notera α^{+} le plus petit cardinal supérieur à α (en 2.3, on avait introduit une notation similaire, mais on l'a abandonnée : le successeur d'un ordinal α est maintenant noté $\alpha + 1$).

Par ailleurs, la borne supérieure d'un ensemble de cardinaux est un cardinal :

PROPOSITION : *Soit* A *un ensemble de cardinaux ; alors* sup A *est un cardinal.*

☹ Si A admet un élément maximum α, alors $\alpha = \sup A$.

Posons $\alpha = \sup A$. Soit β un ordinal strictement inférieur à α ; par définition de la borne supérieure, β n'est pas un majorant de A, et il existe donc un ordinal γ appartenant à A tel que $\gamma > \beta$. Comme γ appartient à A, on a : $\alpha \geqslant \gamma$ et $\text{card}\ \alpha \geqslant \text{card}\ \gamma = \gamma > \beta$. Le cardinal de α est donc strictement supérieur à tout ordinal strictement inférieur à α, ce qui montre que α est un cardinal.

☺

Cela montre en particulier que la classe des cardinaux n'est pas un ensemble : sinon sa borne supérieure en serait un élément maximum, ce qui contredirait le théorème ci-dessus.

4.13 On peut définir par induction une fonction strictement croissante de la classe des ordinaux dans la classe des cardinaux infinis. On utilise habituellement la lettre hébraïque « $\aleph$ » (lire aleph) pour désigner cette fonction :

- $\aleph_0 = \omega$ (le plus petit ordinal infini) ;
- si $\alpha = \beta + 1$ est un ordinal successeur, alors $\aleph_\alpha = \aleph_\beta^+$.
- si α est un ordinal limite, alors $\aleph_\alpha = \sup\{\aleph_\beta\ ;\ \beta < \alpha\}$ (c'est un cardinal d'après la proposition 4.12).

Le fait que la fonction $\aleph$ soit strictement croissante (donc injective) est évident à partir de la définition. Cela montre en particulier que, pour tout ordinal α, $\aleph_\alpha \geqslant \alpha$ (voir lemme 2.6). On voit que, pour tout ordinal α, $\aleph_\alpha$ est un cardinal infini.

On peut montrer aussi que, pour tout cardinal infini λ, il existe un ordinal α tel que $\aleph_\alpha = \lambda$: on a vu que $\aleph_{\lambda+1} > \lambda$, donc il existe un plus petit ordinal α tel que $\aleph_\alpha > \lambda$; α ne peut pas être limite, sinon, par définition de $\aleph_\alpha$, il existerait un ordinal $\gamma < \alpha$ tel que $\aleph_\gamma > \lambda$, contredisant la minimalité de α. Comme α ne peut pas non plus être égal à 0, il existe un ordinal β tel que $\beta + 1 = \alpha$, et

$$\aleph_\beta \leqslant \lambda < \aleph_{\beta+1} = \aleph_\alpha.$$

La cardinalité de λ est donc au plus $\aleph_\beta$, et comme c'est un cardinal, $\aleph_\beta = \lambda$. On voit donc que la fonction $\aleph$ est une bijection strictement croissante de la classe des ordinaux sur la classe des cardinaux infinis.

Supposons momentanément que l'axiome du choix soit vérifié et revenons aux preuves du théorème 4.12. Etant donné un cardinal λ, chacune des preuves nous a fourni un cardinal strictement supérieur : on obtient d'une part le cardinal de 2^λ (abusivement noté 2^λ), et d'autre part le cardinal successeur de λ, noté λ^+. Il est clair que $\lambda^+ \leqslant 2^\lambda$.

Mais ces cardinaux sont-ils égaux ? Cette question ne peut pas être décidée à l'aide des seuls axiomes de ZFC (attendez jusqu'à 5.8 si cette phrase vous paraît sibylline). On a l'habitude d'appeler « **Hypothèse Généralisée du Continu** » (HGC en abrégé et GCH en anglais) la propriété suivante :

(HGC) Pour tout ordinal α, $\aleph_{\alpha+1} = 2^{\aleph_\alpha}$.

L'adjectif « généralisée » vient du fait que le cas où α est égal à **0** est particulièrement important, et est connu sous le nom « **d'Hypothèse du Continu** » (HC, CH en anglais) :

(HC) $\aleph_1 = 2^{\aleph_0}$.

L'hypothèse du continu est équivalente à l'assertion suivante : tout sous-ensemble infini de $\mathbb{R}$ est soit équipotent à $\mathbb{N}$, soit équipotent à $\mathbb{R}$. Rappelons que « le continu » est la cardinalité de $\mathbb{R}$.

4.14 On va maintenant montrer que, en présence de l'axiome du choix, les opérations d'addition et de multiplication sur les cardinaux infinis ne sont pas très intéressantes.

THEOREME : *Pour tout cardinal infini λ :*
1°) $\lambda \,\dot\cup\, \lambda$ est équipotent à λ ;
2°) $\lambda \times \lambda$ est équipotent à λ .

☺ Il suffit de montrer 2°) : en effet, $\lambda \,\dot\cup\, \lambda$ est en bijection avec $\lambda \times 2$. Or $\mathrm{card}(\lambda \times \lambda) \geqslant \mathrm{card}(\lambda \times 2)$ (corollaire 4.3). Donc $\mathrm{card}(\lambda \times \lambda) = \mathrm{card}(\lambda)$ implique bien : $\mathrm{card}(\lambda \,\dot\cup\, \lambda) = \mathrm{card}(\lambda)$.

On raisonne par induction, et on suppose que, pour tout cardinal infini μ strictement inférieur à λ, $\mu \times \mu$ est équipotent à μ. On va définir sur $\lambda \times \lambda$ une relation d'ordre $\leqslant_R$ de la façon suivante : si β, γ, β_1, γ_1 sont des éléments de λ, alors $(\beta,\gamma) \leqslant_R (\beta_1,\gamma_1)$ si et seulement si :

$\sup(\beta,\gamma) < \sup(\beta_1,\gamma_1)$,

ou $\sup(\beta,\gamma) = \sup(\beta_1,\gamma_1)$ et $\beta < \beta_1$,

ou $\sup(\beta,\gamma) = \sup(\beta_1,\gamma_1)$ et $\beta = \beta_1$ et $\gamma \leqslant \gamma_1$.

On laisse au lecteur le soin de vérifier que $\leqslant_R$ est effectivement une relation d'ordre. Montrons que c'est un bon ordre : soit X un sous-ensemble non vide de $\lambda \times \lambda$. On considère :

$X_1 = \{ (\beta,\gamma) \in X \text{ ; pour tout } (\beta_1,\gamma_1) \in X, \sup(\beta,\gamma) \leqslant \sup(\beta_1,\gamma_1) \}$,

c'est-à-dire l'ensemble des éléments (β,γ) de X tels que $\sup(\beta,\gamma)$ soit minimum ; X_1 n'est pas vide, et on considère successivement :

$X_2 = \{ (\beta,\gamma) \in X_1 \text{ ; pour tout } (\beta_1,\gamma_1) \in X_1,\ \beta \leqslant \beta_1 \}$,

et $X_3 = \{ (\beta,\gamma) \in X_2 \text{ ; pour tout } (\beta_1,\gamma_1) \in X_2,\ \gamma \leqslant \gamma_1 \}$.

Alors X_3 n'a qu'un seul élément qui est le plus petit élément de X.

D'après la proposition 3 de 2.6, il existe un ordinal α et un isomorphisme f de $(\alpha,\in)$ sur $(\lambda \times \lambda, \leqslant_R)$. On va voir que cet ordinal α ne peut pas être supérieur à λ. En supposant le contraire, on voit que $\lambda \in \alpha$. Posons $f(\lambda) = (\beta_0,\gamma_0)$; β_0 et γ_0 sont donc des ordinaux appartenant à λ, et $f\restriction_\lambda$ (la restriction de f à λ) est une bijection de λ sur l'ensemble $Y = \{ (\beta,\gamma) \text{ ; } (\beta,\gamma) <_R (\beta_0,\gamma_0) \}$. Posons $\delta_0 = \sup(\beta_0,\gamma_0)$. La cardinalité de δ_0 est strictement inférieure à celle de λ (parce que λ est un cardinal), et, donc, par hypothèse d'induction, il en est de même de la cardinalité de $\delta_0 \times \delta_0$. D'autre part, Y est inclus dans $\delta_0 \times \delta_0$, et, par conséquent, $\text{card}(Y) < \text{card}(\lambda)$. On a bien la contradiction cherchée puisque $f\restriction_\lambda$ est une bijection de λ sur Y.

Cela montre que f est une bijection d'une partie de λ sur $\lambda \times \lambda$: $\text{card}(\lambda \times \lambda) \leqslant \text{card}(\lambda)$. L'inégalité dans l'autre sens est évidente.

☺

COROLLAIRE (AC) : *1°) Si* X *et* Y *sont des ensembles non vides dont l'un au moins est infini, alors :*

$$\text{card}(X \times Y) = \text{card}(X \cup Y) = \sup(\text{card}(X),\text{card}(Y)) .$$

2°) Si $(X_i \text{ ; } i \in I)$ *est une famille d'ensembles et si l'un des* X_i *est infini, alors :* $\text{card}(\bigcup_{i \in I} X_i) \leqslant \sup(\sup\{\text{card}(X_i) \text{ ; } i \in I\}, \text{card}(I))$.

3°) Une réunion dénombrable d'ensembles dénombrables est dénombrable.

☹ 1°) Posons :

$$\lambda = \sup(\text{card}(X),\text{card}(Y)).$$

Il est d'abord clair que l'application identique de X dans lui-même est aussi une injection de X dans $X \cup Y$. Ceci montre que $\text{card}(X) \leqslant \text{card}(X \cup Y)$. Pour la même raison, $\text{card}(Y) \leqslant \text{card}(X \cup Y)$, et donc $\text{card}(X \cup Y) \geqslant \lambda$. Par ailleurs, si y est un point de Y (qui n'est pas vide), l'application qui à $x \in X$ fait correspondre (x,y) est injective de X dans $X \times Y$. On en déduit $\text{card}(X) \leqslant \text{card}(X \times Y)$, et, comme précédemment, $\text{card}(X \times Y) \geqslant \lambda$.

Dans l'autre sens, d'après le corollaire 4.3, on a : $\text{card}(X \times Y) \leqslant \lambda \times \lambda$, et d'après le théorème précédent, $\lambda \times \lambda = \lambda$. On obtient donc $\text{card}(X \times Y) \leqslant \lambda$. Il y a aussi une injection f de $X \cup Y$ dans $X \mathbin{\dot\cup} Y$: si $x \in X$, alors $f(x) = (x,0)$ sinon $f(x) = (x,1)$. Cela montre que :

$$\text{card}(X \cup Y) \leqslant \text{card}(X \mathbin{\dot\cup} Y) \leqslant \lambda + \lambda = \lambda.$$

2°) Posons $X = \bigcup_{i \in I} X_i$ et $\lambda = \sup(\sup\{\text{card}(X_i) \text{ ; } i \in I\}, \text{card}(I))$. Par hypothèse, λ est infini. Pour chaque $x \in X$, l'ensemble $I_x = \{i \in I \text{ ; } x \in X_i\}$ n'est pas vide, donc, par

AC, il existe une application f de X dans I telle que, pour tout $x \in X$, $x \in X_{f(x)}$. D'autre part, pour tout $i \in I$, l'ensemble $\{g\ ;\ g$ est une application injective de X_i dans $\lambda\}$ n'est pas vide (puisque $\mathrm{card}(X_i) \leqslant \lambda$), et donc, en utilisant encore une fois l'axiome du choix, on peut trouver une famille $(g_i\ ;\ i \in I)$ telle que, pour tout $i \in I$, g_i est une application injective de X_i dans λ. On vérifie alors facilement que l'application de X dans $I \times \lambda$ qui à $x \in X$ fait correspondre $(f(x), g_{f(x)}(x))$ est injective, ce qui montre que la cardinalité de X est inférieure ou égale à $\lambda \times \lambda$, qui elle-même est égale à λ.

3°) C'est une conséquence à peu près évidente de 2°). On la signale d'abord parce qu'elle est importante, ensuite pour insister sur le fait que la preuve utilise l'axiome du choix.

☺

REMARQUE : On voit donc que si λ et μ sont deux cardinaux infinis tels que $\lambda > \mu$, alors $\lambda + \mu = \lambda + \lambda$ et $\lambda \times \mu = \lambda \times \lambda$ (voir la remarque après le corollaire 4.3)

Voici une petite propriété fort utile :

PROPOSITION (AC) : *Soient* B *un ensemble infini et* A *un sous-ensemble de* B, *et on suppose que*

$$\mathrm{card}\ A < \mathrm{card}\ B.$$

Alors $\mathrm{card}\ B = \mathrm{card}(B - A)$.

☹ En effet, $B = A \cup (B - A)$. D'après le corollaire 4.14, card B est soit égale à card A, soit égale à card(B - A) (parce qu'elle est égale à sup (card A, card(B - A))). Par hypothèse, l'éventualité card A = card B est impossible.

☺

4.15 On voit donc que la cardinalité de l'union d'une famille d'ensemble est facile à contrôler. Il n'en est pas du tout de même de la cardinalité d'un produit infini. Le théorème suivant, dû à **Kōnig**, donne une indication :

THEOREME (AC) : *Soient* $(X_i\ ;\ i \in I)$ *et* $(Y_i\ ;\ i \in I)$ *deux familles d'ensembles, et on suppose que, pour tout* $i \in I$, $\mathrm{card}(X_i) < \mathrm{card}(Y_i)$. *Alors*

$$\mathrm{card}(\bigcup_{i \in I} X_i) < \mathrm{card}(\prod_{i \in I} Y_i).$$

(Attention : les inégalités sont strictes !)

☹ Posons $X = \bigcup_{i \in I} X_i$ et $Y = \prod_{i \in I} Y_i$, et soit f une application de X dans Y. On va voir que f n'est pas surjective. Pour chaque $x \in X$, $f(x)$ s'écrit sous la forme $(f(x)_i\ ;\ i \in I)$, où, pour tout $i \in I$, $f(x)_i \in Y_i$. Pour chaque $i \in I$, on peut donc définir une application f_i de X_i dans Y_i, par : pour tout $x \in X_i$, $f_i(x) = f(x)_i$. Puisque $\text{card}(X_i) < \text{card}(Y_i)$, l'application f_i n'est pas surjective sur Y_i, et donc, l'ensemble

$$B_i = \{y \in Y_i\ ;\ \text{pour tout } x \in X_i,\ f_i(x) \neq y\}$$

n'est pas vide. En utilisant l'axiome du choix, on voit qu'il existe un élément $b = (b_i\ ;\ i \in I) \in \prod_{i \in I} B_i$. Alors b ne peut pas être dans l'image de f : si on suppose $b = f(x)$, avec $x \in X$, alors il existe $i \in I$ tel que $x \in X_i$, et $f_i(x) = b_i$, ce qui contredit le fait que b_i appartient à B_i.

☺

On verra (exercice 16) des applications du théorème de König.

5. L'AXIOME DE FONDATION ET LE SCHEMA DE REFLEXION

L'axiome de fondation

5.1 Il y a encore au moins une question importante et naturelle dont nous n'avons pas discuté : existe-t-il un ensemble x s'appartenant à lui-même ? L'intuition commune semble être contre une réponse affirmative, mais nous nous garderons bien d'aborder le problème sous cet angle. Comme d'habitude, on adoptera une attitude axiomatique : on va introduire, puis exploiter un nouvel axiome, l'axiome de fondation, qu'on notera AF, dont une conséquence sera en effet qu'il n'existe pas d'ensemble s'appartenant à lui-même. On utilisera cet axiome pour montrer quelques résultats de consistance relative.

• **L'axiome de fondation** : $\forall v_0(\neg v_0 \simeq \emptyset \Longrightarrow \exists v_1(v_1 \in v_0 \wedge v_0 \cap v_1 \simeq \emptyset))$.

On montre d'abord que AF implique :

$$\forall v_0(v_0 \notin v_0).$$

En effet, soit x un ensemble. Alors $\{x\}$ n'est pas vide, donc, d'après AF, il existe un ensemble $y \in \{x\}$ tel que $y \cap \{x\}$ est vide. Or, y ne peut qu'être égal à x, et par conséquent, $x \cap \{x\}$ est vide, ce qui montre bien que $x \notin x$.

La proposition suivante ne sera pas utilisée par la suite. Elle aidera peut-être à mieux saisir la signification de l'axiome de fondation. Elle utilise l'axiome du choix.

PROPOSITION (AC) : *L'axiome de fondation est équivalent à la propriété suivante :*
(∗) *Il n'existe pas de famille* $(a_i\ ;\ i \in \omega)$ *telle que, pour tout* $i \in \omega$, $a_{i+1} \in a_i$.

☺ On montre d'abord que AF implique (∗) (sans axiome du choix) : soit $(a_i\ ;\ i \in \omega)$ une famille indexée par ω, et considérons l'ensemble $A = \{a_i\ ;\ i \in \omega\}$. D'après AF, il existe un élément de A, disons a_n, tel que $a_n \cap A = \emptyset$. Donc $a_{n+1} \notin a_n$.

Supposons réciproquement que AF soit faux. Il existe donc un ensemble non vide x, tel que pour tout élément y de x, $y \cap x$ ne soit pas vide. Avec l'axiome du choix, on voit qu'il existe une application f de x dans lui-même telle que, pour tout $y \in x$, $f(y) \in y \cap x$. Soit a_0 un élément de x. On définit la suite $(a_i\ ;\ i \in \omega)$ par récurrence sur i : pour tout $i \in \omega$, $a_{i+1} = f(a_i)$. On a bien : pour tout $i \in \omega$, $a_{i+1} \in a_i$.
☺

5.2 On va donner une autre propriété équivalente à AF, qui va nous demander un peu plus de travail. On définit par induction sur l'ordinal α, un ensemble V_α par :

$$V_\alpha = \bigcup_{\beta<\alpha} \mathfrak{P}(V_\beta).$$

Ainsi, V_0 qui est l'union de la famille vide, est égal à $\emptyset$. On peut aussi calculer :

$$V_1 = \{\emptyset\},\quad V_2 = \{\emptyset,\{\emptyset\}\},\quad V_3 = \{\emptyset,\{\emptyset\},\{\{\emptyset\}\},\{\emptyset,\{\emptyset\}\}\}\ \text{etc.}$$

On voit aussi que si β et α sont deux ordinaux tels que $\beta < \alpha$, alors $V_\beta \subseteq V_\alpha$ et,

- si α est un ordinal limite, $V_\alpha = \bigcup_{\beta<\alpha} V_\beta$;
- si α est égal à $\beta + 1$, alors $V_\alpha = \mathfrak{P}(V_\beta)$.

Désignons par $\mathcal{V}$ la classe des ensembles x tels qu'il existe un ordinal α tel que $x \in V_\alpha$; pour chaque ensemble x dans $\mathcal{V}$, on appelle **rang de** x et on note rg(x) le plus petit ordinal α tel que $x \in V_\alpha$. On remarque que le rang de x est toujours un ordinal successeur (parce que, si α est un ordinal limite, $V_\alpha = \bigcup_{\beta<\alpha} V_\beta$). Le lecteur pourra aussi montrer par induction que pour tout ordinal α, α appartient à $V_{\alpha+1}$ mais pas à V_α (autrement dit, $\mathrm{rg}(\alpha) = \alpha + 1$).

REMARQUE : Rappelons qu'un ensemble x est transitif si et seulement si, pour tout $y \in x$ et tout $z \in y$, $z \in x$. Pour tout ordinal α, V_α est un ensemble transitif : si $x \in V_\alpha$ et $y \in x$, alors il existe $\beta < \alpha$ tel que $x \subseteq V_\beta$, et donc $y \in V_\beta$. On a montré par dessus le marché que, si x et y sont dans $\mathscr{V}$ et si $x \in y$, alors $rg(x) < rg(y)$.

Tout ensemble x est inclus dans un ensemble transitif : on définit par récurrence sur l'entier n un ensemble x_n de la façon suivante :

- $x_0 = x$;
- pour tout entier n, $x_{n+1} = (\bigcup_{t \in x_n} t) \cup x_n$.

Posons $cl(x) = \bigcup_{n \in \omega} x_n$. Il est d'abord clair que $x \subseteq cl(x)$. D'autre part $cl(x)$ est un ensemble transitif : si $y \in cl(x)$ et $z \in y$, alors il existe un entier n tel que $y \in x_n$ et donc, $z \in x_{n+1}$. De plus, $cl(x)$ est le plus petit ensemble transitif dans lequel x soit inclus : si t est un ensemble transitif et si $x \subseteq t$, alors on voit par induction sur $n \in \omega$ que $x_n \subseteq t$, et donc $cl(x) \subseteq t$. L'ensemble $cl(x)$ s'appelle la **clôture transitive de** x.

THEOREME : *L'axiome de fondation est équivalent à la propriété suivante :*
(**) Pour tout ensemble x, *il existe un ordinal* α *tel que* $x \in V_\alpha$.
(Autrement dit, la classe $\mathscr{V}$ *est l'univers tout entier.)*

☹ On montre d'abord que (**) implique l'axiome de fondation : soit x un ensemble non vide ; il s'agit de trouver un élément y de x tel que $y \cap x = \emptyset$. Par hypothèse, tout ensemble a un rang ; choisissons un élément y de x de rang minimum ; si $t \in y$, alors $rg(t) < rg(y)$ (voir remarque ci-dessus), et par minimalité de $rg(y)$, $t \notin x$.

Voyons la réciproque. On commence par une remarque : si tous les éléments d'un ensemble x appartiennent à $\mathscr{V}$, alors x lui-même appartient à $\mathscr{V}$. En effet, par remplacement, l'image de x par la fonction rg est un ensemble :

$$Y = \{\beta \, ; \text{il existe } y \in x \text{ tel que } rg(y) = \beta\}.$$

Soit $\alpha = \sup Y$. Alors $x \subseteq V_\alpha$, et par conséquent $x \in V_{\alpha+1}$.

Soit x un ensemble quelconque. Posons $y = cl(x)$, et considérons :

$$z = \{t \, ; \, t \in y \text{ et } t \text{ n'est pas dans } \mathscr{V}\}.$$

On va montrer que z est vide, ce qui impliquera que tous les éléments de x sont dans $\mathscr{V}$, et, avec la remarque que l'on vient de faire, que x est dans $\mathscr{V}$. Si z n'était pas vide, alors, par AF, il existerait un élément t de z tel que $t \cap z = \emptyset$. Soit $u \in t$. D'abord, $u \notin z$ ($t \cap z = \emptyset$) ; ensuite, parce que y est transitif, $u \in y$, et donc, par définition de z, u est dans $\mathscr{V}$. Autrement dit, tous les éléments de t sont dans $\mathscr{V}$, et donc t est dans $\mathscr{V}$, ce qui est contradictoire avec $t \in z$.

☺

Quelques résultats de consistance relative

5.3 Les **théorèmes de consistance relative** ont la forme suivante : étant données deux théories T_1 et T_2 (très souvent, T_2 contient T_1), alors, si T_1 n'est pas contradictoire, il en est de même de T_2. Dans les exemples que nous allons donner, T_1 sera la théorie ZF. Le principe des démonstrations de ces théorèmes est simple : à partir d'un modèle de T_1, on construit un modèle de T_2.

Une remarque en passant : on peut préférer démontrer des théorèmes de cohérence relative qui s'exprimeraient ainsi : si on ne peut pas démontrer de contradiction à partir de T_1, alors on ne peut pas démontrer de contradiction à partir de T_2. Evidemment, le théorème de complétude implique qu'il n'y a pas de différence entre ces deux formulations. Cependant, la seconde formulation présente l'avantage, écrasant lorsqu'on s'intéresse aux fondements des mathématiques, de pouvoir s'exprimer à l'aide de notions appartenant aux mathématiques finies (les formules sont des suites finies de symboles, les preuves des suites finies de formules, etc.). En fait, les preuves que nous allons présenter permettent, bien que ce ne soit pas évident a priori, de déduire un algorithme qui, à partir d'une démonstration formelle d'une formule notoirement fausse F (par exemple $0=1$) dans T_2 donne une démonstration formelle de F dans T_1. N'insistons pas plus sur ce point.

On peut remarquer que l'ensemble des entiers, muni des fonctions adéquates, est un modèle des axiomes de Peano ; on a donc montré :

• Si ZF n'est pas contradictoire, alors l'arithmétique de Peano, $\mathscr{P}$, n'est pas contradictoire non plus.

Cela montre, en passant, à cause du second théorème d'incomplétude de Gödel (chapitre 6), qu'on ne peut pas espérer avoir un théorème de consistance absolue, par exemple : ZF n'est pas contradictoire. Pour en terminer avec ces relations entre ZF et $\mathscr{P}$, disons que ZF est beaucoup plus fort que $\mathscr{P}$: la consistance de $\mathscr{P}$ peut s'exprimer par une formule de la théorie des ensembles, et cette formule est démontrable à partir de ZF (parce que la structure $\mathbb{N}$ est un point de $\mathscr{U}$, et le fait que ce soit un modèle de $\mathscr{P}$ est un théorème de ZF) ; la consistance de ZF peut s'exprimer par une formule de l'arithmétique (parce que, de toute évidence, ZF est une théorie récursive), mais, en revanche, cette formule n'est pas démontrable dans $\mathscr{P}$ (sinon, avec le théorème de consistance cité ci-dessus, on en déduirait que $\mathscr{P}$ démontre sa propre consistance, ce que le théorème de Gödel interdit).

5.4 Si $\mathscr{A}$ est une classe (ou un ensemble, considéré comme la classe de ses éléments), on considérera la sous-structure de $\mathfrak{U}$ dont la base est $\mathscr{A}$, que l'on notera $<\mathscr{A},\in>$. C'est parmi ces structures que l'on va trouver les modèles des différentes théories dont on montre la consistance.

Soient $D[v_0]$ une formule et $\mathscr{A}$ la classe des ensembles x satisfaisant $D[x]$. Etant donnée une formule F, on définit la formule $F^{\mathscr{A}}$, appelée **relativisée de F à $\mathscr{A}$**, par induction (intuitive) sur la complexité de F :

– si F est atomique, alors $F^{\mathscr{A}} = F$;

– si F est égale à $\neg G$, alors $F^{\mathscr{A}} = \neg G^{\mathscr{A}}$;

– si F est égale à $(G \,\alpha\, H)$, où α est un connecteur propositionnel binaire, alors $F^{\mathscr{A}} = (G^{\mathscr{A}} \,\alpha\, H^{\mathscr{A}})$;

– si F est égale à $\exists vG$, où v est un symbole de variable, alors :

$$F^{\mathscr{A}} = \exists v(D[v] \wedge G^{\mathscr{A}}) ;$$

– si F est égale à $\forall vG$, où v est un symbole de variable, alors :

$$F^{\mathscr{A}} = \forall v(D[v] \Rightarrow G^{\mathscr{A}}).$$

On montre alors sans peine, toujours par induction intuitive sur la hauteur de F que, pour toute formule $F[v_1,v_2,\ldots,v_n]$ et pour tous $x_1, x_2, \ldots,x_n$ dans $\mathscr{A}$,

$$\mathfrak{U} \models F^{\mathscr{A}}[x_1,x_2,\ldots,x_n] \text{ si et seulement si } <\mathscr{A},\in> \models F[x_1,x_2,\ldots,x_n].$$

On va avoir besoin, à plusieurs reprises, des quelques remarques qui suivent :

1°) Si $\mathscr{A}$ est une classe transitive, alors $<\mathscr{A},\in>$ satisfait l'axiome d'extensionnalité. Soient en effet x et y deux ensembles distincts dans $\mathscr{A}$. Par extensionnalité dans $\mathscr{U}$, il existe un ensemble z qui appartient à l'un, disons par exemple x, mais pas à l'autre. Puisque z appartient à x, que x est dans $\mathscr{A}$ et que $\mathscr{A}$ est transitif, z est dans $\mathscr{A}$, et il existe un élément de $\mathscr{A}$, à savoir z, qui appartient à x mais pas à y : c'est ce qu'il nous fallait pour montrer l'extensionnalité dans $\mathscr{A}$.

2°) Si α est un ordinal et x et y appartiennent à V_α, alors $\{x,y\}$ appartient à $V_{\alpha+1}$. Si δ est un ordinal limite et si x et y appartiennent à V_δ, alors il existe un ordinal $\alpha < \delta$ tel que x et y appartiennent à V_α, et donc $\{x,y\}$ appartient à V_δ ; on en déduit que, si δ est un ordinal limite, alors $<V_\delta,\in>$ satisfait l'axiome de la paire. De même $<\mathscr{V},\in>$ satisfait l'axiome de la paire.

3°) Si $x \in V_\alpha$, alors $\mathfrak{P}(x) \subseteq V_{\alpha+1}$ et $\mathfrak{P}(x) \in V_{\alpha+2}$: si δ est un ordinal limite, $<V_\delta,\in>$ satisfait l'axiome des parties.

4°) Pour tout α, $<V_\alpha,\in>$ satisfait l'axiome de la réunion : soit $x \in V_\alpha$; alors le rang de x est un ordinal successeur, donc de la forme $\beta + 1$; si $y \in \bigcup x$, alors il existe $z \in x$ tel que $y \in z$. On a vu (remarque 5.2) que $rg(z) \leqslant \beta$ et $rg(y) < \beta$. Cela implique : $\bigcup x \subseteq V_\beta$ et $\bigcup x \in V_\alpha$.

5°) Pour tout ordinal α et pour tout $a \in V_\alpha$, on a :

$$<V_\alpha,\in> \models On[a] \text{ si et seulement si } \mathfrak{U} \models On[a].$$

La vérification ne pose aucun problème : on voit qu'un élément a de V_α est transitif si et seulement si il l'est dans $<V_\alpha,\in>$, puis que les différentes propriétés qui font que la relation d'appartenance est un bon ordre sont vraies dans $\mathfrak{U}$ si et seulement si elles le sont dans $<V_\alpha,\in>$. De même, on montre que :

$$\mathfrak{U} \models \mathrm{On}[a] \text{ si et seulement si } <\mathcal{V},\in> \models \mathrm{On}[a].$$

Il y a bien d'autres propriétés qui passent ainsi de $\mathfrak{U}$ à $<V_\alpha,\in>$ ou à $<\mathcal{V},\in>$. Par exemple, le lecteur pourra tout aussi facilement montrer que si α est un ordinal limite et $a \in V_\alpha$, alors les trois propriétés suivantes sont équivalentes :

$\mathfrak{U} \models$ a est un cardinal ;

$<V_\alpha,\in> \models$ a est un cardinal ;

$<\mathcal{V},\in> \models$ a est un cardinal.

5.5 THEOREME : *Si* ZF *est consistant, alors* ZF + AF *est consistant.*

☹ Soient $\mathcal{U}$ un modèle de ZF et $\mathcal{V}$ la classe des ensembles x de $\mathcal{U}$ satisfaisant la formule :

$$F[x] = \text{il existe un ordinal } \alpha \text{ tel que } x \in V_\alpha.$$

On va montrer que $<\mathcal{V},\in>$ est un modèle de ZF + AF.

L'axiome d'extensionnalité, les axiomes de la paire, de la réunion, et des parties ont déjà été montrés dans les remarques qui précèdent.

• Les axiomes de remplacement :

Soient donc x un élément de $\mathcal{V}$ et $G[v_0,v_1]$ une formule qui, dans $<\mathcal{V},\in>$, est fonctionnelle en v_0, autrement dit telle que :

$$<\mathcal{V},\in> \models \forall v_0 \forall v_1 \forall v_2((G[v_0,v_1] \wedge G[v_0,v_2]) \Longrightarrow v_1 \simeq v_2)).$$

Alors, $H = F[v_0] \wedge F[v_1] \wedge G^{\mathcal{V}}$ est fonctionnelle en v_0 (dans $\mathfrak{U}$). Soit b l'image de x par la fonction que cette formule définit :

$$b = \{z\ ;\ (\exists y \in x)H[y,z]\}.$$

Alors b est dans $\mathcal{V}$ (parce que tous ses éléments sont dans $\mathcal{V}$), et c'est ce qu'il fallait démontrer.

• L'axiome de fondation : soit x un ensemble qui se trouve dans $\mathcal{V}$; alors tous les éléments de x sont aussi dans $\mathcal{V}$. Soit y un élément de x, dont le rang α est minimum. Alors, si u est un élément de y, son rang est strictement plus petit que α (remarque 5.2), et u n'appartient pas à x : $x \cap y$ est vide.

• L'axiome de l'infini : ω est dans $\mathcal{V}$. On a vu que c'est un ordinal de $\mathcal{V}$, et il est facile de voir que, dans $\mathcal{V}$, il n'est ni vide ni successeur. On peut voir que c'est, dans $\mathcal{V}$, le premier ordinal infini.

☺

REMARQUE 1 : Dans la démonstration qui précède, on pourrait croire qu'il est évident que l'axiome de fondation est satisfait dans $\mathcal{V}$. Ceci n'est pas tout à fait vrai : la classe $\mathcal{V}$ est définie par une formule que l'on appelle $F[v_0]$. Alors il faut se rendre compte que F a même signification dans $\mathcal{U}$ et dans $\mathcal{V}$, autrement dit que :

$$\mathfrak{U} \models \forall v_0(F[v_0] \Longleftrightarrow F^{\mathscr{V}}[v_0]).$$

Si, dans $\mathscr{V}$, on définit par induction sur α les ensembles W_α par :

$W_0 = \emptyset$;

$W_\alpha = \bigcup_{\beta<\alpha} \mathfrak{P}(W_\alpha)$;

alors, il est facile de vérifier que, pour tout ordinal α, $V_\alpha = W_\alpha$. Ceci, avec le théorème 5.2 (et le fait que les ordinaux sont les mêmes dans $\mathfrak{U}$ et dans $\mathscr{V}$), donne une autre démonstration du fait que $<\mathscr{V}, \epsilon>$ satisfait l'axiome de fondation.

REMARQUE 2 : Si on suppose que $\mathfrak{U}$ est un modèle de ZFC, alors $<\mathscr{V},\epsilon>$ est un modèle de ZFC + AF. En effet, si $X = (x_i ; i \in I)$ est une famille d'ensembles non vides se trouvant dans $\mathscr{V}$, alors I lui-même est dans $\mathscr{V}$ (c'est le domaine de définition de X, considéré comme une application ; donc I est inclus dans $\bigcup\bigcup X$) ; de même chacun des x_i est dans $\mathscr{V}$. Cela montre que n'importe quel élément de $\prod_{i \in I} x_i$ est dans $\mathscr{V}$.

5.6 Le second théorème de consistance relative que nous allons voir montre que l'axiome de l'infini est indispensable :

THEOREME : *Si* ZF *est consistant, alors* $ZF^- + \neg Inf$ *est aussi consistant.*

☺ On va montrer que V_ω est un modèle de $ZF^- + \neg Inf$. L'extensionnalité, les axiomes de la paire, de la réunion et des parties ont déjà été traités.

Passons à l'axiome de remplacement. Remarquons que, pour tout entier n, V_n est un ensemble fini (démonstration évidente par récurrence sur n). Donc, tous les éléments de V_ω sont des ensembles finis. Réciproquement, si x est un ensemble fini tel que tous les éléments de x appartiennent à V_ω, alors x appartient à V_ω : en effet, $X = \{rg(y) ; y \in x\}$, l'image de x par la fonction rg, est un ensemble (remplacement) fini (proposition 3 de 4.7), et, par hypothèse, c'est un sous-ensemble de ω. Si $n = \sup X$, $x \in V_{n+1}$.

Soient x un élément de V_ω et $F[v_0,v_1]$ une formule qui, dans $<V_\omega,\epsilon>$ est fonctionnelle en v_0 :

$$<V_\omega,\epsilon> \models \forall v_0 \forall v_1 \forall v_2((F[v_0,v_1] \wedge F[v_0,v_2]) \Longrightarrow v_1 \simeq v_2).$$

Alors, $G = v_0 \in V_\omega \wedge v_1 \in V_\omega \wedge F^{V_\omega}$ est fonctionnelle en v_0 (dans $\mathfrak{U}$). Soit b l'image de x par la fonction que cette formule définit dans $\mathfrak{U}$:

$$b = \{ z ; (\exists y \in x)G[y,z] \}.$$

Alors b est un ensemble fini (parce qu'il existe une surjection d'une partie de x sur b), dont tous les éléments appartiennent à V_ω. On vient de voir que cela implique que $b \in V_\omega$.

Il est facile de montrer que V_ω ne satisfait pas l'axiome de l'infini : si x est un élément de V_ω, x est fini et il n'existe pas, ni dans $\mathcal{U}$, ni a fortiori dans V_ω, d'application de x dans x qui soit injective et non bijective (contrairement à ce qui se passe dans tout modèle de ZF, voir remarque 4.8).
☺

REMARQUE : il est très facile de montrer que l'axiome de fondation est vrai dans V_ω ; l'axiome du choix y est aussi vrai (même s'il n'est pas vrai dans $\mathfrak{U}$), mais c'est un peu plus délicat à démontrer.

Cardinaux inaccessibles

5.7 Dans cette sous-section, on va travailler dans ZFC.

DEFINITIONS : *Soit λ un cardinal.*

i) On dit que λ est **fortement limite** *si, pour tout cardinal μ strictement inférieur à λ, le cardinal de 2^μ est aussi strictement inférieur à λ.*

ii) On dit que λ est **régulier** *si, pour tout sous-ensemble X de λ de cardinalité strictement inférieure à λ, $\sup(X) < \lambda$.*

iii) On dit que λ est **inaccessible** *s'il est strictement supérieur à $\aleph_0$, régulier et fortement limite.*

Voyons quelques exemples. Pour tout ordinal α, définissons par induction un cardinal $\beth_\alpha$:

- $\beth_0 = \aleph_0$;
- si δ est un ordinal limite, alors $\beth_\delta = \bigcup_{\alpha\in\delta} \beth_\alpha$;
- $\beth_{\alpha+1} = 2^{\beth_\alpha}$.

(Le symbole « $\beth$ » se lit beth ; c'est la deuxième lettre de l'alphabet hébraïque.)

On montre sans peine que, pour tout ordinal α, $\aleph_\alpha \leqslant \beth_\alpha$ (par induction sur α), et si on suppose l'hypothèse généralisée du continu (voir 4.13), alors $\aleph_\alpha = \beth_\alpha$.

Il est clair que $\beth_\omega$ est un cardinal fortement limite. En revanche, il n'est pas régulier : en effet, si on pose :

$$X = \{\beth_n \,;\, n \in \omega\},$$

alors X est dénombrable, donc de cardinalité strictement inférieure à $\beth_\omega$, et pourtant $\sup(X) = \beth_\omega$.

Par ailleurs, pour tout ordinal α, $\aleph_{\alpha+1}$ est un cardinal régulier (pour montrer cela, l'axiome du choix est nécessaire ; on peut montrer que ce fait n'est pas une conséquence de ZF) : soit X un sous-ensemble de $\aleph_{\alpha+1}$ de cardinalité au plus $\aleph_\alpha$. Tous les éléments de X ont une cardinalité au plus égale à $\aleph_\alpha$, et donc, $\bigcup_{x \in X} x$, qui est égal à $\sup(X)$ a une cardinalité au plus égale à $\aleph_\alpha$ (corollaire 4.14, 2°)).

Evidemment, $\aleph_{\alpha+1}$ n'est pas fortement limite, puisque $2^{\aleph_\alpha} \geqslant \aleph_{\alpha+1}$. On n'a donc pas d'exemple de cardinaux inaccessibles, et cela n'est pas très étonnant puisque :

THEOREME : *Si* ZFC *est consistant, alors* ZFC + « *il n'existe pas de cardinaux inaccessibles* » *est aussi consistant.*

⊖ Soit $\mathfrak{U}$ un modèle de ZFC. On veut trouver un modèle de ZFC qui ne contienne pas de cardinaux inaccessibles. On peut supposer qu'il y a, dans $\mathcal{U}$, un cardinal inaccessible κ, sinon il n'y a rien à faire. On va montrer que $< V_\kappa, \in >$ est un modèle de ZFC, et que, si κ est le premier cardinal inaccessible dans $\mathcal{U}$, alors il n'y a pas de cardinaux inaccessibles dans V_κ.

Les axiomes d'extensionnalité, de la paire, de la réunion et des parties se montrent comme d'habitude.

Pour le schéma de remplacement, on montre d'abord que si $x \in V_\kappa$, alors $\text{card}(x) < \kappa$. Si $x \in V_\kappa$, il existe $\alpha < \kappa$ tel que x soit inclus dans V_α ; il suffit donc de montrer que si $\alpha < \kappa$, alors $\text{card}(V_\alpha) < \kappa$. Cela se fait par induction sur α. C'est évident si $\alpha = 0$. Si $\alpha = \beta + 1$, alors $\text{card}(V_\alpha) = 2^{\text{card}(V_\beta)}$; par hypothèse d'induction, $\text{card}(V_\beta) < \kappa$, donc, parce que κ est fortement limite, $\text{card}(V_\alpha) < \kappa$. Si α est un ordinal limite, alors $V_\alpha = \bigcup_{\beta<\alpha} V_\beta$, et $\text{card}(V_\alpha) = \sup(\sup\{\text{card}(V_\beta) ; \beta < \alpha\}, \alpha)$. Avec l'hypothèse d'induction et le fait que κ est régulier, on voit que $\text{card}(V_\alpha) < \kappa$.

Supposons maintenant que x soit un ensemble de cardinalité strictement inférieure à κ et dont tous les éléments appartiennent à V_κ. Alors x appartient à V_κ : on considère $X = \{\alpha \in \kappa ; \text{ il existe } y \in x \text{ tel que } \alpha \text{ soit le rang de } y\}$. L'ensemble X est l'image de x par la fonction rang, donc sa cardinalité est strictement inférieure à κ (proposition 4.11). Par régularité de κ, $\beta = \sup(X)$ est aussi strictement inférieur à κ, et x est inclus dans V_β. Cela montre que $x \in V_{\beta+1}$.

Pour montrer que les axiomes de remplacement sont vrais dans V_κ, il suffit d'adapter la démonstration qui nous a servi pour V_ω (remplacer V_ω par V_κ et « fini » par « de cardinalité inférieure à κ »). L'axiome de l'infini est vérifié par $< V_\kappa, \in >$ parce que ω est un ordinal infini dans $< V_\kappa, \in >$.

Pour se convaincre que V_κ satisfait AC, il suffit d'observer que, κ étant

inaccessible, la remarque 2 de 5.5 reste valable lorsqu'on y remplace $\mathscr{V}$ par V_κ.

Reste à voir que, si κ est le premier cardinal inaccessible, alors :

$<V_\kappa, \in> \models$ il n'existe pas de cardinaux inaccessibles.

On se souvient ici que les cardinaux de V_κ sont les mêmes que ceux de $\mathfrak{U}$. Parce κ est le plus petit cardinal inaccessible, on sait déjà que :

$\mathfrak{U} \models$ il n'y a pas de cardinaux inaccessibles appartenant à V_κ,

et il suffit donc de montrer que, pour tout $x \in V_\kappa$:

$\mathfrak{U} \models x$ est un cardinal inaccessible si et seulement si $<V_\kappa, \in> \models x$ est un cardinal inaccessible.

On vérifie sans difficulté que, pour tout élément x de V_κ, si x est un cardinal,

$\mathfrak{U} \models x$ est régulier si et seulement si $<V_\kappa, \in> \models x$ est régulier,

et $\mathfrak{U} \models x$ est fortement limite si et seulement si $<V_\kappa, \in> \models x$ est fortement limite.

☺

5.8 Il y a d'autres théorèmes de consistance relative. Les plus célèbres sont : Si ZF est consistant, alors les théories suivantes le sont aussi : ZFC , ZFC + HGC (Gödel), ZF + ¬AC, ZFC + ¬HC (Cohen) (voir le livre de Krivine, « Théorie axiomatique des ensembles », PUF).

Le schéma de réflexion

5.9 Dans cette sous-section, on travaille dans ZF + AF. **Le schéma de réflexion** est la collection des formules pouvant s'écrire :

$$\forall v_0 \forall v_1 \ldots \forall v_n \exists \alpha(\alpha \text{ est un ordinal} \wedge v_0 \in V_\alpha \wedge v_1 \in V_\alpha \wedge \ldots \wedge v_n \in V_\alpha \wedge (F[v_0,v_1,\ldots,v_n] \Longleftrightarrow F^{V_\alpha}[v_0,v_1,\ldots,v_n])).$$

où n est un entier intuitif et $F[v_0,v_1,\ldots,v_n]$ est une formule de $\mathscr{L}$.

DEFINITION : *Soit* $F[v_0,v_1,\ldots,v_n]$ *une formule de* $\mathscr{L}$ *et* A *un ensemble. On dit que* F *se* ***reflète*** *dans* A *si*

$$\mathfrak{U} \models \forall v_0 \forall v_1 \ldots \forall v_n((v_0 \in A \wedge v_1 \in A \wedge \ldots \wedge v_n \in A) \Longrightarrow (F[v_0,v_1,\ldots,v_n] \Longleftrightarrow F^A[v_0,v_1,\ldots,v_n])).$$

Autrement dit, $F[v_0,v_1,\ldots,v_n]$ se reflète dans A si et seulement si, pour tous éléments $a_0,a_1,\ldots,a_n$ de A, $\mathfrak{U} \models F[a_0,a_1,\ldots,a_n]$ si et seulement si $<A, \in> \models F[a_0,a_1,\ldots,a_n]$.

Le schéma de réflexion exprime donc que, pour toute formule F, il existe un ordinal α tel que F se reflète dans V_α.

Il résulte immédiatement de la définition que, si F_1 et F_2 se reflètent toutes les deux dans A, alors il en est de même de $\neg F_1$, $F_1 \wedge F_2$, $F_1 \vee F_2$, $F_1 \Longrightarrow F_2$ et $F_1 \Longleftrightarrow F_2$.

THEOREME : *Pour toute formule* $F[v_0,v_1,\ldots,v_n]$ *de* $\mathcal{L}$ *on a :*

$$\mathfrak{U} \models \forall v_0 \forall v_1 \ldots \forall v_n \exists \alpha (\alpha \text{ est un ordinal} \wedge v_0 \in V_\alpha \wedge v_1 \in V_\alpha \wedge \ldots \wedge v_n \in V_\alpha \wedge (F[v_0,v_1,\ldots,v_n] \Longleftrightarrow F^{V_\alpha}[v_0,v_1,\ldots,v_n])).$$

(Autrement dit, le schéma de réflexion est conséquence de ZF + AF.)

On a donc un théorème de ZF + AF pour chaque formule F. Tel qu'il est exprimé ci-dessus (pour toute formule F ...), ce n'est pas une formule de $\mathcal{L}$.

☺ On va montrer que, si F est une formule, et si β est un ordinal, alors il existe un ordinal $\alpha > \beta$ tel que F se reflète dans V_α. Cela démontrera bien le théorème (a_0, a_1, ... a_n étant fixés, il suffira de choisir l'ordinal β de sorte que V_β contienne tous ces points). On a d'abord besoin du lemme suivant :

LEMME : *Soient* F *une formule et* $(X_n \, ; \, n \in \omega)$ *une suite croissante (pour l'inclusion) d'ensembles. On suppose que, pour tout* $n \in \omega$ *et pour toute sous-formule* G *de* F, G *se reflète dans* X_n. *Alors* F *se reflète dans* $X = \bigcup_{n \in \omega} X_n$.

☺ La démonstration se fait par induction intuitive sur la hauteur de F. Si F est atomique, c'est évident, puisque F se reflète dans n'importe quel ensemble. Supposons maintenant que $F = F_1 \wedge F_2$. On voit que F_1 et F_2 sont des sous-formules de F, donc, par hypothèse, elles se reflètent dans X_n, pour tout $n \in \omega$. Il découle de l'hypothèse d'induction que F_1 et F_2 se reflètent dans X, et on a déjà remarqué que cela implique que $F_1 \wedge F_2$ se reflète dans X. Les autres connecteurs propositionnels se traitent exactement de la même façon.

Il ne reste plus que le cas des quantificateurs. On va traiter, par exemple le cas où F est de la forme $\exists v_0 G[v_0,v_1,\ldots,v_k]$. Comme G est une sous-formule de F, G se reflète dans chacun des X_n, et, par hypothèse d'induction, G se reflète dans X. Supposons d'abord que $a_1,a_2,\ldots,a_k$ soient des éléments de X et que :

$$<X,\in> \models \exists v_0 G[v_0,a_1,\ldots,a_k].$$

Il existe donc un élément a_0 de X tel que :

$$<X,\in> \models G[a_0,a_1,\ldots,a_k],$$

et, puisque G se reflète dans X,

$$\mathfrak{U} \models G[a_0,a_1,\ldots,a_k] \quad \text{et} \quad \mathfrak{U} \models \exists v_0 G[v_0,a_1,\ldots,a_k].$$

Réciproquement, supposons que $a_1,\ldots,a_k$ soient des éléments de X et que :

$$\mathfrak{U} \models \exists v_0 G[v_0,a_1,\ldots,a_k].$$

Alors il existe un élément $n \in \omega$ tel que X_n contienne $a_1,\ldots,a_k$ (remarquez qu'ici, k est un entier intuitif alors que n est un entier au sens de $\mathfrak{U}$). Du fait que F se reflète dans X_n, on déduit :

$$<X_n,\in> \models \exists v_0 G[v_0,a_1,\ldots,a_k],$$

et donc, il existe a_0 dans X_n tel que :

$$(X_n,\in) \models G[a_0,a_1,\ldots,a_k].$$

On utilise maintenant le fait que G se reflète dans X_n, puis dans X pour déduire :

$$\mathfrak{U} \models G[a_0,a_1,\ldots,a_k] \;,\; <X,\in> \models G[a_0,a_1,\ldots,a_k] \text{ et enfin } <X,\in> \models \exists v_0 G[v_0,a_1,\ldots,a_k].$$

☺

Pour achever la démonstration, il suffit de montrer la propriété (*) suivante :

(*) | pour toute formule F et pour tout ordinal β, il existe un ordinal α supérieur à β tel que F et toutes ses sous-formules se reflètent dans V_α,

par induction intuitive sur la hauteur de F. Le cas où F est atomique est évident (prendre $\alpha=\beta$), de même que le cas où $F=\neg G$ (une formule se reflète dans un ensemble si et seulement si sa négation se reflète dans cet ensemble). On va traiter, par exemple, le cas où $F=F_1 \wedge F_2$ (les autre connecteurs binaires se traitent exactement de la même façon). On définit, par induction sur $n \in \omega$, une suite croissante d'ordinaux α_n de la façon suivante :

- $\alpha_0=\beta$;
- si n est pair et non nul, alors α_n est le plus petit ordinal supérieur à α_{n-1} tel que F_1 et toutes ses sous-formules se reflètent dans V_{α_n} (un tel ordinal existe par hypothèse d'induction) ;
- si n est impair, alors α_n est le plus petit ordinal supérieur à α_{n-1} tel que F_2 et toutes ses sous-formules se reflètent dans V_{α_n} (même remarque).

Remarquez que, pour pouvoir définir la suite $(\alpha_n \;;\; n \in \omega)$ par induction, il faut s'être persuadé auparavant que, si F est une formule fixée de $\mathscr{L}$, il existe une formule $G[v_0]$ de $\mathscr{L}$ telle que, pour tout ensemble x, G[x] est équivalent à « x est un ordinal et F et toutes ses sous-formules se reflètent dans V_x ».

Posons $\alpha=\sup\{\alpha_n \;;\; n \in \omega\}$. On voit alors que V_α est l'union de la famille $(V_{\alpha_n} \;;\; n \in \omega$ et n est pair) ; d'après le lemme, F_1 et toutes ses sous-formules se reflètent dans V_α. Mais V_α est aussi la réunion de la famille $(V_{\alpha_n} \;;\; n \in \omega$ et n est impair), et F_2 et toutes ses sous-formules se reflètent aussi dans V_α. En conséquence, F et toutes ses

sous-formules se reflètent dans V_α.

Passons, pour terminer, au cas où F est égale à $\exists v_0 G[v_0,v_1,...,v_k]$. On prouve d'abord : pour tout ordinal γ, il existe un ordinal δ tel que :

$$\mathfrak{U} \models \forall v_1 \forall v_2 ... \forall v_k((v_1 \in V_\gamma \wedge v_2 \in V_\gamma \wedge ... \wedge v_k \in V_\gamma \wedge \exists v_0 G[v_0,v_1,...,v_k]) \Longrightarrow \exists v_0(v_0 \in V_\delta \wedge G[v_0,v_1,...,v_k])).$$

On considère à cet effet la formule suivante $H[w,\alpha]$: s'il existe $v_0,v_1,v_2,...,v_k$ tels que $w = (v_1,v_2,...,v_k)$ et $G[v_0,v_1,...,v_k]$, alors α est le plus petit ordinal tel qu'il existe u satisfaisant $u \in V_\alpha$ et $G[u,v_1,...,v_k]$; sinon, $\alpha = \emptyset$.

On voit donc que la formule H définit une fonction, et, par remplacement, l'image de l'ensemble des k-uples d'éléments de V_γ est un ensemble Y. Il suffit de choisir δ de sorte que V_δ contienne Y.

On définit alors par induction une suite $(\alpha_n ; n \in \omega)$ de la façon suivante :

- $\alpha_0 = \beta$;
- si n est pair et non nul, alors α_n est le plus petit ordinal supérieur à α_{n-1} tel que G et toutes ses sous-formules se reflètent dans V_{α_n} (un tel ordinal existe par hypothèse d'induction) ;
- si n est impair, alors α_n est le plus petit ordinal tel que :

$$\forall v_1 \forall v_2 ... \forall v_k((v_1 \in V_{\alpha_{n-1}} \wedge v_2 \in V_{\alpha_{n-1}} \wedge ... \wedge v_k \in V_{\alpha_{n-1}} \wedge \exists v_0 G[v_0,v_1,...,v_k]) \Longrightarrow \exists v_0(v_0 \in V_{\alpha_n} \wedge G[v_0,v_1,...,v_k])).$$

Soit α la borne supérieure de l'ensemble $\{\alpha_n ; n \in \omega\}$. Alors, comme précédemment, V_α est l'union de la famille $(V_{\alpha_n} ; n \in \omega$ et n est pair), et, d'après le lemme, G et toutes ses sous-formules se reflètent dans V_α. Il reste à montrer que F lui-même se reflète dans V_α.

Supposons d'abord que $a_1,a_2,...,a_k$ appartiennent à V_α et que :

$$\langle V_\alpha, \in \rangle \models \exists v_0 G[v_0,a_1,a_2,...,a_k].$$

Il existe alors un élément a_0 de V_α tel que :

$$\langle V_\alpha, \in \rangle \models G[a_0,a_1,a_2,...,a_k],$$

et, parce que G se reflète dans V_α,

$$\mathfrak{U} \models G[a_0,a_1,a_2,...,a_k] \text{ et } \mathfrak{U} \models \exists v_0 G[v_0,a_1,a_2,...,a_k].$$

Réciproquement, supposons que :

$$\mathfrak{U} \models \exists v_0 G[v_0,a_1,a_2,...,a_k].$$

On sait qu'il existe un entier n, que l'on peut supposer pair, tel que $a_1,a_2,...,a_k$ appartiennent à V_{α_n} ; par définition de α_{n+1}, il existe un élément a_0 de $V_{\alpha_{n+1}}$ tel que :

$$\mathfrak{U} \models G[a_0,a_1,a_2,...,a_k],$$

et, parce que G se reflète dans V_α,

$$\langle V_\alpha, \in \rangle \models G[a_0,a_1,a_2,...,a_k] \text{ et } \langle V_\alpha, \in \rangle \models \exists v_0 G[v_0,a_1,a_2,...,a_k].$$

☺

5.10 On va terminer ce chapitre par une application du théorème 5.9 :

PROPOSITION : *Si la théorie ZF est consistante, alors elle n'est pas finiment axiomatisable.*

☹ On raisonne par l'absurde ; si ZF est finiment axiomatisable, il en est de même de ZF + AF : soit F une formule de $\mathscr{L}$ équivalente à ZF + AF. on travaille dans un modèle $\mathfrak{U}$ de ZF + AF (qui est consistante d'après le théorème 5.5). D'après le théorème 5.9, il existe un ordinal α tel que :

$$<V_\alpha, \in> \models F ;$$

et donc

$$\mathfrak{U} \models F^{V_\alpha}.$$

Revenons un instant à la définition de la relativisée d'une formule (5.4). Deux faits découlent assez facilement de cette définition : premièrement, il existe une formule $G[v_0]$ de $\mathscr{L}$ tel que, pour tout ensemble A, F^A est équivalente à $G[A]$; deuxièmement, si $A \subseteq B$, alors $(F^A)^B = F^B$.

Il y a donc des ordinaux β satisfaisant $G[V_\beta]$. Considérons donc le plus petit d'entre eux, que l'on appellera γ. Comme $<V_\gamma, \in>$ est un modèle de ZF + AF, le schéma de réflexion y est vrai. Donc :

$$<V_\gamma, \in> \models \text{il existe un ordinal } \delta \text{ tel que } F^{V_\delta}.$$

Mais on a vu en 5.4 que les ordinaux de $<V_\gamma, \in>$ sont les ordinaux inférieurs à γ, et on voit aussi sans peine (cf remarque 1 de 5.5) que, pour tout $x \in V_\gamma$,

$$<V_\gamma, \in> \models x \in V_\delta \text{ si et seulement si } \mathfrak{U} \models x \in V_\delta.$$

Cela montre que :

$$\mathfrak{U} \models (F^{V_\delta})^{V_\gamma},$$

et, puisque $(F^{V_\delta})^{V_\gamma} = F^{V_\delta}$, $<V_\delta, \in>$ est un modèle de F, ce qui contredit la minimalité de γ.

☺

EXERCICES

Dans tous les exercices ci-dessous, on se place, sauf précision contraire, dans un univers $\mathfrak{U}$ *modèle de* ZF.

1. Les notions d'entier naturel, d'appartenance, de fonction, etc., qui interviennent ici sont intuitives : il ne s'agira pas de celles de l'univers $\mathfrak{U}$. On les utilisera pour construire un univers satisfaisant certains des axiomes de ZF.

On désigne par W l'ensemble des parties finies de $\mathbb{N}$.

a) Soit φ une bijection de $\mathbb{N}$ sur W et soit ε_φ la relation binaire définie sur $\mathbb{N}$ par : quels que soient les entiers x et y,

$$x \; \varepsilon_\varphi \; y \text{ si et seulement si } x \in \varphi(y).$$

Montrer que l'univers $\mathfrak{M}_\varphi = <\mathbb{N}, \varepsilon_\varphi>$ satisfait tous les axiomes de ZF à l'exception de l'axiome de l'infini. Montrer que si, pour tous x, y $\in \mathbb{N}$, x $\in \varphi$(y) implique x < y, alors $\mathfrak{M}_\varphi$ satisfait aussi l'axiome de fondation.

b) Montrer que l'application ζ qui à A $\in$ W fait correspondre $\sum_{a \in A} 2^a$ (étant entendu que $\zeta(\emptyset) = 0$) est une bijection de W sur $\mathbb{N}$. Montrer que $\mathfrak{M}_\zeta$ est un modèle de ZF^- et de AF.

c) Trouver une bijection φ de $\mathbb{N}$ sur W telle que $\mathfrak{M}_\varphi$ ne satisfasse pas AF.

2. Montrer que la classe On' définie dans $\mathfrak{U}$ par la formule :

$$\forall y((y \subseteq x \wedge \neg y = x \wedge y \text{ est transitif}) \Longrightarrow y \in x)$$

est la classe des ordinaux.

3. Soient x un ensemble et Γ(x) la classe des ordinaux subpotents à x.

Montrer que Γ(x) est un ordinal, que c'est le plus petit ordinal non subpotent à x, et que c'est un cardinal. On l'appelle **cardinal d'Hartog de** x.

Caractériser Γ(x) lorsque $\mathfrak{U}$ satisfait l'axiome du choix.

4. Cet exercice est consacré à quelques énoncés équivalents à l'axiome du choix.

Une **fonction de choix** sur un ensemble a est une application φ de l'ensemble des parties non vides de a dans a telle que, pour toute partie non vide x $\subseteq$ a, φ(x) $\in$ x.

Montrer que AC est équivalent (moyennant ZF) à chacun des énoncés suivants :

a) Pour tout ensemble a, il existe au moins une fonction de choix sur a.

b) Quels que soient les ensembles x et y et l'application surjective g de x dans y, il existe une application h de y dans x telle que $g \circ h$ soit l'application identique de y dans y.

c) Pour tout ensemble a dont les éléments sont non vides et disjoints deux à deux, il existe un ensemble b dont l'intersection avec chacun des éléments de a est un singleton.

d) Pour tous ensembles a et b, a est subpotent à b ou b est subpotent à a.

(Pour l'équivalence entre AC et d), on pourra utiliser l'exercice 3.)

La propriété d) est connue sous le nom de **trichotomie**, car elle peut aussi s'exprimer ainsi : étant données deux classes cardinales λ et μ, une et une seule des trois situations suivantes se produit :

$$\bullet\ \lambda = \mu \quad ; \quad \bullet\ \lambda < \mu \quad ; \quad \bullet\ \mu < \lambda .$$

Plus simplement, la trichotomie est vérifiée si et seulement si l'ordre sur les classes cardinales est un ordre total.

5. Montrer que, dans la théorie ZF + AF, chacun des trois énoncés suivants est équivalent à l'axiome du choix :

a) Pour tout ensemble x bien ordonnable, l'ensemble $\mathfrak{P}(x)$ est bien ordonnable.

b) Pour tout ordinal α, $\mathfrak{P}(\alpha)$ est bien ordonnable.

c) Tout ensemble totalement ordonnable est bien ordonnable.

6. Montrer, sans utiliser l'axiome du choix, que, pour tout ensemble non vide a, les propriétés suivantes sont équivalentes :

(1) a contient un sous-ensemble dénombrable ;

(2) a contient un sous-ensemble dénombrable b tel que a et $a - b$ soient équipotents ;

(3) pour tout ensemble dénombrable b, a et $a \cup b$ sont équipotents ;

(4) pour tout ensemble fini x, a et $a \cup x$ sont équipotents ;

(5) pour tout sous-ensemble fini x de a, a et $a - x$ sont équipotents ;

(6) il existe un entier $n \in \omega$, non nul, tel que, pour tout sous-ensemble x de a subpotent à n, a et $a - x$ soient équipotents ;

(7) il existe un entier $n \in \omega$, non nul, tel que, pour tout ensemble x de cardinal n, a et $a \cup x$ soient équipotents ;

(8) pour tout t, a et $a \cup \{t\}$ sont équipotents ;

(9) il existe un élément $t \in a$ tel que a et $a - \{t\}$ soient équipotents ;

(10) il existe une partie de a, non vide et distincte de a, équipotente à a ;

(11) il existe une partie $b \subsetneq a$, non vide et distincte de a, telle que a soit subpotent à b.

7. Déterminer le cardinal de chacun des ensembles suivants :

$x_1 = \{f \in \mathbb{N}^{\mathbb{N}} ; (\forall n \in \mathbb{N})(\forall p \in \mathbb{N})(n < p \Longrightarrow f(n) < f(p))\}$;
$x_2 = \{f \in \mathbb{N}^{\mathbb{N}} ; (\exists p \in \mathbb{N})(\forall n \in \mathbb{N})(f(n) \leqslant p)\}$;
$x_3 = \{f \in \mathbb{Q}^{\mathbb{N}} ; (\forall n \in \mathbb{N})(\forall p \in \mathbb{N})(n < p \Longrightarrow f(n) < f(p))\}$;
$x_4 = \{f \in \mathbb{Q}^{\mathbb{N}} ; (\exists p \in \mathbb{Q})(\forall n \in \mathbb{N})(f(n) \leqslant p)\}$;
$x_5 = x_3 \cap x_4$;
$x_6 = \{f \in \mathbb{Q}^{\mathbb{N}} ; (\exists n \in \mathbb{N})(\forall p \in \mathbb{N})(n \leqslant p \Longrightarrow f(n) = f(p))\}$;
$x_7 = \{f \in \mathbb{R}^{\mathbb{N}} ; (\forall r \in \mathbb{R})(\exists n \in \mathbb{N})(f(n) \geqslant r)\}$

8. Déterminer le cardinal de chacun des ensembles suivants :

E_0 = l'ensemble des suites de nombres rationnels ($\mathbb{Q}^{\mathbb{N}}$) ;
E_1 = l'ensemble des suites de nombres réels ($\mathbb{R}^{\mathbb{N}}$) ;
E_2 = l'ensemble des suites de rationnels qui convergent vers 0 ;
E_3 = l'ensemble des suites de rationnels convergentes ;
E_4 = l'ensemble des suites de rationnels bornées ;
E_5 = l'ensemble des suites de rationnels non bornées ;
E_6 = l'ensemble des applications de $\mathbb{Q}$ dans $\mathbb{R}$ ($\mathbb{R}^{\mathbb{Q}}$) ;
E_7 = l'ensemble des applications continues de $\mathbb{R}$ dans $\mathbb{R}$;
E_8 = l'ensemble des intervalles ouverts de $\mathbb{R}$;
E_9 = l'ensemble des ouverts de $\mathbb{R}$ (pour la topologie usuelle).

9. Déterminer le cardinal de chacun des ensembles suivants :

$a_1 = \{f \in \omega^\omega ; (\forall n \in \omega)(\forall p \in \omega)(f(n) \leqslant p)\}$;
$a_2 = \{f \in \omega^\omega ; (\forall n \in \omega)(\exists p \in \omega)(f(n) \leqslant p)\}$;
$a_3 = \{f \in \omega^\omega ; (\exists n \in \omega)(\forall p \in \omega)(f(n) \leqslant p)\}$;
$a_4 = \{f \in \omega^\omega ; (\exists n \in \omega)(\exists p \in \omega)(f(n) \leqslant p)\}$;
$a_5 = \{f \in \omega^\omega ; (\exists p \in \omega)(\forall n \in \omega)(f(n) \leqslant p)\}$;
$a_6 = \{f \in \omega^\omega ; (\forall p \in \omega)(\exists n \in \omega)(f(n) \leqslant p)\}$;
$b_1 = \{f \in \omega^\omega ; (\forall n \in \omega)(\forall p \in \omega)(f(n) \geqslant p)\}$;
$b_2 = \{f \in \omega^\omega ; (\forall n \in \omega)(\exists p \in \omega)(f(n) \geqslant p)\}$;
$b_3 = \{f \in \omega^\omega ; (\exists n \in \omega)(\forall p \in \omega)(f(n) \geqslant p)\}$;
$b_4 = \{f \in \omega^\omega ; (\exists n \in \omega)(\exists p \in \omega)(f(n) \geqslant p)\}$;
$b_5 = \{f \in \omega^\omega ; (\exists p \in \omega)(\forall n \in \omega)(f(n) \geqslant p)\}$;
$b_6 = \{f \in \omega^\omega ; (\forall p \in \omega)(\exists n \in \omega)(f(n) \geqslant p)\}$.

10. On suppose que l'univers satisfait l'axiome de choix. On considère deux ensembles infinis a et b, de cardinaux respectifs λ et μ. On suppose $\lambda > \mu$ (inégalité stricte). On se donne une application injective g de b dans a. On demande de déterminer le cardinal de chacun des ensembles suivants :

$y_1 = \{f \in b^a ; \operatorname{card}(\overline{f}(a)) = 1\}$;
$y_2 = \{f \in b^a ; (\forall x \in \mathfrak{P}(a))(\operatorname{card}(\overline{f}(x)) \leqslant 1)\}$;
$y_3 = \{f \in b^a ; \operatorname{card}(\overline{f}^{-1}(b)) = \lambda\}$;
$y_4 = \{f \in b^a ; \operatorname{card}(\overline{f}(a)) = 2\}$;
$y_5 = a - \overline{g}(b)$;
$y_6 = \{f \in b^a ; (\forall y \in b)(f(g(y)) = y)\}$;
$y_7 = \{f \in b^a ; \operatorname{card}(\overline{f}(a)) = \mu\}$.

(On rappelle que, si $f \in b^a$, $\overline{f}$ et $\overline{f}^{-1}$ désignent respectivement l'application image directe et l'application image réciproque induites par f de $\mathfrak{P}(a)$ dans $\mathfrak{P}(b)$ et de $\mathfrak{P}(b)$ dans $\mathfrak{P}(a)$.)

11. On suppose que l'univers satisfait l'axiome du choix. On considère un ensemble a infini et on appelle λ son cardinal. On pose :

$$\mathfrak{P}^*(a) = \{x \in \mathfrak{P}(a) ; \operatorname{card}(x) = \operatorname{card}(a - x)\}.$$

a) Montrer que, pour tout entier $n \in \omega$, si $n \neq 0$, on peut trouver des ensembles $a_1, a_2, \ldots, a_n$, tous de cardinal λ, qui constituent une partition de a (c'est-à-dire : qui sont deux à deux disjoints et tels que $\bigcup_{1 \leqslant i \leqslant n} a_i = a$).

b) Déterminer le cardinal de chacun des éléments de $\mathfrak{P}^*(a)$.

c) En utilisant la question a) lorsque $n = 3$, déterminer le cardinal de $\mathfrak{P}^*(a)$.

d) Montrer que, pour tout ensemble $a_1 \in \mathfrak{P}^*(a)$, il existe une bijection f de a sur a telle que, pour tout $x \in a$, $f(x) = x$ si et seulement si $x \in a_1$.

e) Déterminer le cardinal de l'ensemble des bijections de a sur a.

f) Soit b un élément de $\mathfrak{P}^*(a)$. Déterminer le cardinal de l'ensemble des bijections de a sur a dont la restriction à b est l'identité sur b.

g) Quel est le cardinal de l'ensemble des applications injectives de a dans $\mathfrak{P}(a)$?

12. On suppose que l'univers satisfait l'axiome du choix. On considère un cardinal infini λ, un ordinal α, et une famille d'ensembles $(X_\beta)_{\beta \in \alpha}$ indexée par α telle que :

- pour tout $\beta \in \alpha$, $\operatorname{card}(X_\beta) < \lambda$;
- pour tous $\beta \in \alpha$ et $\gamma \in \alpha$, si $\beta < \gamma$, alors $X_\beta \subseteq X_\gamma$.

Montrer que $\operatorname{card}(\bigcup_{\beta \in \alpha} X_\beta) \leqslant \lambda$.

13. On suppose que l'univers satisfait l'axiome du choix. Montrer que, pour toute famille $(\lambda_\alpha)_{\alpha \in \kappa}$ de cardinaux non nuls, indexée par un cardinal infini κ, on a :

$$\sum_{\alpha \in \kappa} \lambda_\alpha = \sup(\kappa, \sup_{\alpha \in \kappa}(\lambda_\alpha)).$$

14. On suppose que l'univers satisfait l'axiome du choix.

Soit μ un cardinal infini. On définit, par induction sur les entiers, une suite de cardinaux $(\lambda_n)_{n\in\omega}$:

$$\lambda_0 = \mu \; ; \; \text{pour tout } n \in \omega, \; \lambda_{n+1} = 2^{\lambda_n}.$$

On pose $\lambda = \sum_{n\in\omega} \lambda_n$.

a) Montrer que $\lambda^{\mu} = \mu^{\lambda} = \lambda^{\lambda} = 2^{\lambda}$.

b) Montrer que, pour tout cardinal γ,

- si $\aleph_0 \leqslant \gamma \leqslant \lambda$, alors $\lambda^{\aleph_0} = \lambda^{\gamma} = \lambda^{\lambda}$;
- si $\gamma \geqslant \lambda$, alors $\lambda^{\gamma} = 2^{\gamma}$.

c) Montrer qu'il existe des cardinaux α, β, γ et δ tels que :

$$\alpha < \beta \; , \; \gamma < \delta \; \text{ et } \; \alpha^{\gamma} = \beta^{\delta}.$$

15. Soient α et β deux ordinaux. Par définition, α est **cofinal à** β si et seulement si il existe une application f de β dans α, strictement croissante, non strictement majorée. (Ce qui veut dire que :

- quels que soient les ordinaux γ et δ appartenant à β, si $\gamma < \delta$, alors $f(\gamma) < f(\delta)$,

et
- pour tout ordinal $\xi \in \alpha$, il existe $\gamma \in \beta$ tel que $f(\gamma) \geqslant \xi$.)

a) Montrer que la (méta)relation « être cofinal à » définie sur la classe On est réflexive, transitive et non symétrique. Déterminer les ordinaux cofinaux à 1.

b) Montrer que, pour tout ordinal α, la classe des ordinaux β tels que α soit cofinal à β est un ensemble non vide.

Le plus petit ordinal appartenant à cet ensemble est appelé **cofinalité de** α et noté $\mathrm{cof}(\alpha)$. Tout ordinal α tel que $\mathrm{cof}(\alpha) = \alpha$ est appelé ordinal **régulier**.

Montrer que, pour tout ordinal α, $\mathrm{cof}(\alpha) \leqslant \alpha$ et $\mathrm{cof}(\alpha)$ est un ordinal régulier.

c) Montrer que, quels que soient les ordinaux α et β, $\beta < \mathrm{cof}(\alpha)$ si et seulement si toute application de β dans α est strictement majorée dans α.

d) Montrer que tout ordinal régulier est un cardinal. Montrer que, pour tout cardinal λ, λ est un ordinal régulier si et seulement si c'est un cardinal régulier au sens de la définition 5.7, ii.

e) On suppose que l'univers satisfait l'axiome du choix. Montrer que, pour tout ordinal α, $\aleph_{\alpha+1}$ est régulier. Montrer que si α est un ordinal limite, $\mathrm{cof}(\aleph_\alpha) = \mathrm{cof}(\alpha)$.

f) Déterminer le premier ordinal (respectivement : le premier cardinal) strictement supérieur à ω qui soit cofinal à ω.

16. On suppose que l'univers satisfait l'axiome du choix. On se servira des notions et des résultats de l'exercice précédent.

a) Montrer que, pour tout cardinal infini λ, $\lambda^{\mathrm{cof}(\lambda)} > \lambda$ (utiliser le théorème de König).

b) Montrer que $\mathrm{card}(2^{\omega})$ n'est pas cofinal à ω.

c) On suppose que l'univers satisfait l'hypothèse généralisée du continu (HGC), c'est-à-dire que, pour tout ordinal α, $2^{\aleph_\alpha} = \aleph_{\alpha+1}$.

Soit λ un cardinal infini. Montrer que, pour tout cardinal μ autre que 0, on a :

$$\lambda^{\mu} = \begin{cases} \lambda & \text{si } \mu < \mathrm{cof}(\lambda) \ ; \\ 2^{\lambda} & \text{si } \mathrm{cof}(\lambda) \leqslant \mu \leqslant \lambda \ ; \\ 2^{\mu} & \text{si } \lambda < \mu. \end{cases}$$

17. Soit Φ une fonction (définissable) définie sur la classe On des ordinaux, à valeurs dans On, strictement croissante. On dit que Φ est **continue en un ordinal limite** α si $\Phi(\alpha) = \sup_{\beta \in \alpha} \Phi(\beta)$. On dit que Φ est **continue** si elle est continue en tout ordinal limite.

Un ordinal α tel que $\Phi(\alpha) = \alpha$ est appelé **point fixe de** Φ.

a) Montrer que toute fonction Φ strictement croissante de On dans On possède la propriété suivante : pour tout ordinal α, $\Phi(\alpha) \geqslant \alpha$.

b) Montrer que, si Φ est une fonction strictement croissante de On dans On, continue en tout ordinal cofinal à ω, alors, pour tout ordinal α, Φ admet un point fixe supérieur à α.

c) Montrer que, si Φ et Ψ sont deux fonctions strictement croissantes de On dans On, continues en tout ordinal cofinal à ω, alors, pour tout ordinal α, Φ et Ψ admettent un point fixe commun supérieur à α.

d) On suppose que l'univers satisfait l'axiome du choix. Montrer que, pour tout ordinal α, il existe un ordinal $\beta > \alpha$ tel que $\mathrm{card}(V_\beta) = \aleph_\beta = \beta$.

18. On suppose que l'univers satisfait HGC et AC (en fait, on peut montrer que l'axiome du choix est vrai dans tout modèle de ZF + HGC).

a) La fonction de On dans On qui, à chaque ordinal α, associe $\aleph_0^{\aleph_\alpha}$ est-elle continue en tout ordinal limite ? (voir l'exercice 17 pour la définition de la continuité). Même question pour la fonction qui, à α, associe $\aleph_\alpha^{\aleph_0}$.

b) Soit δ un ordinal. La fonction qui, à chaque ordinal α, associe l'ordinal $\delta + \alpha$ (somme ordinale) est-elle continue en tout ordinal limite ? Même question pour les fonctions qui, à α, associent respectivement : $\alpha + \delta$, $\alpha.\delta$, $\delta.\alpha$ (il s'agit toujours des opérations ordinales).

19. Montrer que l'axiome de fondation est équivalent (moyennant les axiomes de ZF) au schéma d'axiome suivant :

$$\exists v_0 F[v_0] \Longrightarrow \exists v_0 (F[v_0] \wedge \forall v_1 (v_1 \in v_0 \Longrightarrow \neg F[v_1]))$$

(où F est une formule à une variable libre quelconque du langage $\{\in, \simeq\}$).

20. Dans cet exercice, on suppose que l'axiome du choix est vérifié. Soit λ un cardinal régulier (voir définition 5.7) non dénombrable. On dit qu'un sous-ensemble X de λ est **clos cofinal** si :

1) il est clos : pour tout sous-ensemble X_0 de X qui est tel que $\mathrm{card}(X_0) < \lambda$, $\sup X_0 \in X$ (remarquez que $\sup X_0$ est un ordinal strictement inférieur à λ parce que λ est régulier).

2) il est cofinal : pour tout $\alpha \in \lambda$, il existe $\beta \in X$ tel que $\beta > \alpha$.

a) Montrer que les sous-ensembles clos cofinaux de λ forment une base de filtre sur λ (voir chapitre 2, 5.12).

b) Montrer que, si I est un ensemble de cardinalité strictement inférieure à λ et si $(X_i\,;\, i \in I)$ est une famille de sous-ensembles clos cofinaux de λ, alors $\bigcap_{i \in I} X_i$ est clos cofinal.

c) On dit qu'un sous-ensemble Y de λ est **stationnaire** s'il rencontre tous les ensembles clos cofinaux. Montrer que les trois propriétés suivantes sont équivalentes :

1) il existe deux ensembles stationnaires disjoints ;

2) il existe au moins un ensemble stationnaire qui ne contient pas d'ensemble clos cofinal.

3) le filtre engendré par les ensembles clos cofinaux n'est pas un ultrafiltre.

d) Soit $X = (X_\alpha\,;\, \alpha \in \lambda)$ une suite de sous-ensembles de λ. L'ensemble :

$$\{\alpha \in \lambda\,;\, \alpha \in X_\alpha\}$$

est appelé l'**intersection diagonale** de X et est noté $\Delta(X)$. Montrer que, si X satisfait les trois conditions suivantes :

(1) pour tout $\alpha \in \lambda$, X_α est clos cofinal ;

(2) pour tous α et $\beta \in \lambda$, si $\alpha \in \beta$, alors $X_\beta \subseteq X_\alpha$;

(3) pour tout $\alpha \in \lambda$, α ordinal limite, $X_\alpha = \bigcap_{\beta \in \alpha} X_\beta$,

alors $\Delta(X)$ est clos cofinal.

e) Montrer le théorème suivant (**théorème de Fodor**) :

THEOREME : *Soit* f *une application de* λ *dans* λ *telle que* $\{\alpha \in \lambda\,;\, f(\alpha) < \alpha\}$ *soit stationnaire. Alors il existe* $\alpha \in \lambda$ *tel que* $f^{-1}(\alpha)$, *l'image réciproque de* α *par* f, *est stationnaire.*

f) On suppose que $\lambda \geqslant \aleph_2$. Montrer que l'ensemble des ordinaux de cofinalité $\aleph_0$ (voir exercice 15) est stationnaire. Montrer que l'ensemble des ordinaux de cofinalité $\aleph_1$ est aussi stationnaire et disjoint du précédent.

g) La question f) montre que, pour tout cardinal régulier λ strictement supérieur à $\aleph_1$, les conditions de la question c) sont vérifiées. Le raisonnement que nous proposons dans cette question montre que ces conditions sont encore vérifiées pour $\lambda = \aleph_1$ (d'ailleurs cette preuve fonctionne pour n'importe quel cardinal successeur).

Pour chaque ordinal α dénombrable et non nul, soit f_α une application surjective de ω sur α, et, pour tout $n \in \omega$, soit h_n l'application de $\aleph_1$ dans $\aleph_1$ définie par : $h_n(0) = 0$ et $h_n(\alpha) = f_\alpha(n)$ si $\alpha \neq 0$. Montrer que, pour tout $n \in \omega$, il existe $\beta_n \in \aleph_1$ et un sous-ensemble stationnaire Y_n de $\aleph_1$ tels que : pour tout $\gamma \in Y_n$, $f_\gamma(n) = \beta_n$. Montrer qu'il existe un entier n tel que Y_n ne soit pas clos cofinal.

21. Montrer que, si α est un ordinal limite strictement supérieur à ω, alors $< V_\alpha , \in >$ est un modèle de la théorie Z.

b) En déduire que, si Z est une théorie consistante, les axiomes de ZF ne sont pas conséquence de ceux de Z.

22. On suppose que l'univers satisfait l'axiome du choix.

On considère la classe $\mathscr{W}$ des ensembles x tels que cl(x) (la clôture transitive de x, voir 5.2) est dénombrable. Montrer que $< \mathscr{W} , \in >$ est un modèle des axiomes de ZF à l'exception de l'axiome des parties.

23. Montrer, en utilisant directement un argument diagonal, que l'intervalle réel]0,1] n'est pas dénombrable.

Chapitre 8

Un peu de théorie des modèles

La théorie des modèles est l'étude de la classe des modèles d'une théorie donnée. On a déjà rencontré au moins deux théorèmes qui allaient dans cette direction : le théorème de complétude et le puissant théorème de compacité qui affirment tous les deux que, sous certaines conditions, cette classe n'est pas vide.

La notion centrale de ce chapitre et du genre de théorie des modèles dont on donne ici les bases est la notion de sous-structure élémentaire. Intuitivement, $\mathfrak{M}$ *est une sous-structure élémentaire de* $\mathfrak{N}$ *si, évidemment,* $\mathfrak{M}$ *est une sous-structure de* $\mathfrak{N}$ *et si, pour toute suite finie* s *d'éléments de* $\mathfrak{M}$*, et pour toute propriété* F[s] *qui peut s'exprimer à l'aide d'une formule du premier ordre, il est équivalent de vérifier que* s *satisfait* F *dans* $\mathfrak{M}$ *ou qu'elle la satisfait dans* $\mathfrak{N}$*. C'est de cette notion que l'on s'occupera dans les deux premières sections, avec comme résultats importants les théorèmes de Lowenheim-Skolem, et leur corollaire qui veut qu'une théorie dénombrable ayant un modèle infini en ait un en toute cardinalité infinie.*

On passe ensuite aux théorèmes d'interpolation et de définissabilité. Il vaut la peine de s'arrêter sur la signification de ce dernier théorème. Lorsqu'on veut formaliser une théorie, il faut commencer par fixer le langage, ce qui revient à décider quelles notions doivent être considérées comme primitives, les autres devant se définir à partir d'elles (par exemple, dans le cas de l'arithmétique, 0,S,+ *et* × *suffisent ; on peut ensuite définir la relation d'ordre, les nombres premiers, etc.). Mais comment être sûr de ne pas avoir introduit de symboles inutiles ? Le théorème de définissabilité donne un critère sémantique qui répond à la question.*

La quatrième section est consacrée aux produits réduits et aux ultraproduits, qui sont des opérations de nature algébrique permettant de définir une L*-structure à partir d'autres* L*-structures. Les ultraproduits sont particulièrement importants et fournissent une preuve purement algébrique du théorème de compacité. A la section 5, on démontrera quelques théorèmes du type : une théorie* T *est équivalente à une théorie de telle ou telle forme si et seulement si la classe de ses modèles est close pour telle ou telle opération. Ces théorèmes sont appelés théorèmes de préservation. On examinera notamment la préservation par sous-structure, union de chaîne et produit réduit. Enfin, dans la dernière section, on étudiera les modèles dénombrables d'une théorie* $\aleph_0$*-catégorique, c'est-à-dire d'une théorie dont tous les modèles dénombrables sont isomorphes.*

1. SOUS-STRUCTURES ET EXTENSIONS ELEMENTAIRES

Sous-structures élémentaires

1.1 On adoptera dans tout ce chapitre la convention suivante : on utilisera des lettres gothiques $\mathfrak{M}$, $\mathfrak{N}$, etc. pour désigner des structures, et on utilisera les lettres latines correspondantes (M, N, etc.) pour les ensembles sous-jacents à ces structures. On supposera systématiquement que le langage contient l'égalité et que les structures sont égalitaires. La définition qui suit est très importante et sera présente dans tout le chapitre.

DEFINITION : *Soient* L *un langage,* $\mathfrak{M}$ *une* L*-structure et* $\mathfrak{N}$ *une sous-structure de* $\mathfrak{M}$ *; on dit que* $\mathfrak{N}$ *est une* ***sous-structure élémentaire de*** $\mathfrak{M}$ *(ou, d'une façon équivalente, que* $\mathfrak{M}$ *est une* ***extension élémentaire de*** $\mathfrak{N}$*) si, pour toute formule* $F[v_1,v_2,...,v_n]$ de L *et tous élements* $a_1, a_2, ..., a_n$ *de* N, *on a :*

$$\mathfrak{M} \models F[a_1,a_2,...,a_n] \text{ si et seulement si } \mathfrak{N} \models F[a_1,a_2,...,a_n].$$

On écrira $\mathfrak{N} \prec \mathfrak{M}$ *pour : «* $\mathfrak{N}$ *est une sous-structure élémentaire de* $\mathfrak{M}$ *».*

Remarquons que, pour que $\mathfrak{N}$ soit simplement une sous-structure de $\mathfrak{M}$, il faut que la même condition formelle, mais portant seulement sur les formules F atomiques (ou, ce qui revient au même, sur les formules sans quantificateur), soit vérifiée. La première question qui vient à l'esprit est de savoir s'il y a des sous-structures qui ne sont pas élémentaires ; en voici quelques exemples :

• Dans le langage des groupes, $<\mathbb{Z},0,+>$ est une sous-structure de $<\mathbb{Q},0,+>$ qui n'est pas élémentaire. En effet, la formule $\forall v_0 \exists v_1(v_1 + v_1 \simeq v_0)$ est satisfaite dans $\mathbb{Q}$ mais pas dans $\mathbb{Z}$.

• Dans le même langage, $<2\mathbb{Z},0,+>$, le groupe des entiers relatifs pairs, est une sous-structure de $<\mathbb{Z},0,+>$ et, de plus, on voit que ces deux structures sont isomorphes et satisfont donc les mêmes formules sans paramètre. Pourtant, la formule $\exists v_0(v_0 + v_0 \simeq 2)$ est satisfaite dans $\mathbb{Z}$ mais pas dans $2\mathbb{Z}$, qui n'est donc pas une

sous-structure élémentaire de $\mathbb{Z}$. Contrairement au premier exemple, on a besoin ici d'un paramètre de la petite structure (à savoir 2) pour trouver une formule vraie dans une structure mais pas dans l'autre.

• Dans le langage des corps, $\mathbb{Q}$ n'est pas une sous-structure élémentaire de $\mathbb{R}$: la formules $\exists v_0(v_0 \times v_0 \simeq 2)$ est satisfaite dans $\mathbb{R}$ et pas dans $\mathbb{Q}$. De même $\mathbb{R}$ n'est pas une sous-structure élémentaire de $\mathbb{C}$, comme la formule $\exists v_0(v_0 \times v_0 \simeq -1)$ en témoigne (ici, on n'utilise pas de paramètres, contrairement aux apparences).

• Dans le langage des ordres, $[0,1]$ n'est pas une sous-structure élémentaire de $[0,2]$: la formule $\forall v_0(v_0 \leqslant 1)$ est satisfaite dans la première mais pas dans la seconde.

1.2 Voici un rappel de définitions de la section 5 du chapitre 3.

DEFINITION : *Soit* $\mathfrak{M}$ *une* L-structure ; *on appelle théorie complète de* $\mathfrak{M}$ *et on note* $\mathrm{Th}(\mathfrak{M})$ *la théorie* :

$$\mathrm{Th}(\mathfrak{M}) = \{ F \text{ ; } F \text{ est une formule close de } L \text{ et } \mathfrak{M} \models F \}.$$

Si $\mathfrak{M}$ *et* $\mathfrak{N}$ *sont deux* L-*structures, on dit que* $\mathfrak{M}$ *et* $\mathfrak{N}$ *sont* ***élémentairement équivalentes*** *si* $\mathrm{Th}(\mathfrak{M}) = \mathrm{Th}(\mathfrak{N})$. *Dans ce cas, on écrira* $\mathfrak{M} \equiv \mathfrak{N}$.

Il est clair que, conformément au vocabulaire, $\mathrm{Th}(\mathfrak{M})$ est toujours une théorie complète, et que deux structures isomorphes sont élémentairement équivalentes. Des définitions, il découle immédiatement que, si $\mathfrak{M} \prec \mathfrak{N}$, alors $\mathfrak{M} \equiv \mathfrak{N}$. L'exemple de $<2\mathbb{Z},0,+>$ dans $<\mathbb{Z},0,+>$ montre qu'il est très possible que $\mathfrak{N}$ soit une sous-structure de $\mathfrak{M}$ élémentairement équivalente à $\mathfrak{M}$ sans en être une sous-structure élémentaire.

REMARQUE : Il découle aussi des définitions que :

• si $\mathfrak{M}_1 \prec \mathfrak{M}_2$ et $\mathfrak{M}_2 \prec \mathfrak{M}_3$, alors $\mathfrak{M}_1 \prec \mathfrak{M}_3$;

• si $\mathfrak{M}_1 \prec \mathfrak{M}_3$, $\mathfrak{M}_1 \subseteq \mathfrak{M}_2$ et $\mathfrak{M}_2 \prec \mathfrak{M}_3$, alors $\mathfrak{M}_1 \prec \mathfrak{M}_2$.

1.3 Il est en général assez difficile de montrer qu'une sous-structure est élémentaire. On va dans l'exemple suivant exposer une technique très utile pour ce genre de problème.

EXEMPLE : **les ordres denses sans extrémités**. On considère la théorie T suivante dans le langage ne comportant qu'un seul symbole de relation binaire $<$:

(i) $\forall v_0(\neg v_0 < v_0)$

(ii) $\forall v_0 \forall v_1((v_0 < v_1 \Longleftrightarrow \neg v_1 < v_0) \vee v_0 \simeq v_1)$
(iii) $\forall v_0 \forall v_1 \forall v_2((v_0 < v_1 \wedge v_1 < v_2) \Longrightarrow v_0 < v_2)$
(iv) $\forall v_0 \exists v_1(v_0 < v_1)$
(v) $\forall v_0 \exists v_1(v_1 < v_0)$
(vi) $\forall v_0 \forall v_1 \exists v_2(v_0 < v_1 \Longrightarrow (v_0 < v_2 \wedge v_2 < v_1))$.

Les trois premiers axiomes expriment que $<$ est une relation d'ordre total, les deux suivants qu'il n'y a pas d'élément maximum ni d'élément minimum, et le dernier que l'ordre est dense, c'est-à-dire qu'entre deux éléments distincts, il y en a toujours un troisième. Il est clair qu'un modèle de T est nécessairement infini. On va montrer que, si $\mathfrak{M}$ et $\mathfrak{N}$ sont deux modèles de T et $\mathfrak{M} \subseteq \mathfrak{N}$, alors $\mathfrak{M} \prec \mathfrak{N}$. Il s'agit là d'une propriété extrêmement forte de la théorie T (voir l'exercice 8). On va d'abord montrer deux lemmes :

LEMME 1 : *Soient* $a_1,a_2,\ldots,a_n \in M$, $b_1,b_2,\ldots,b_n \in N$, *et on suppose que ces deux suites satisfont respectivement dans* $\mathfrak{M}$ *et* $\mathfrak{N}$, *les mêmes formules atomiques, autrement dit : pour tous* i *et* $j \in \{1,2,\ldots,n\}$,

$\mathfrak{M} \models a_i \simeq a_j$ *si et seulement si* $\mathfrak{N} \models b_i \simeq b_j$;

et $\mathfrak{M} \models a_i < a_j$ *si et seulement si* $\mathfrak{N} \models b_i < b_j$.

Alors :

pour tout $a_0 \in M$, *il existe* $b_0 \in N$ *tel que : pour tous* i *et* $j \in \{0,1,2,\ldots,n\}$,

$\mathfrak{M} \models a_i \simeq a_j$ *si et seulement si* $\mathfrak{N} \models b_i \simeq b_j$;

et $\mathfrak{M} \models a_i < a_j$ *si et seulement si* $\mathfrak{N} \models b_i < b_j$;

et pour tout $b_0 \in N$, *il existe* $a_0 \in M$ *tel que : pour tous* i *et* $j \in \{0,1,2,\ldots,n\}$,

$\mathfrak{M} \models a_i \simeq a_j$ *si et seulement si* $\mathfrak{N} \models b_i \simeq b_j$;

et $\mathfrak{M} \models a_i < a_j$ *si et seulement si* $\mathfrak{N} \models b_i < b_j$.

☺ On se donne le point a_0 et on cherche b_0. On distingue plusieurs cas :

• a_0 est plus grand (au sens de l'ordre de $\mathfrak{M}$) que tous les a_i (pour $1 \leqslant i \leqslant n$). On choisit alors b_0 dans N plus grand (au sens de l'ordre de $\mathfrak{N}$) que tous les b_i (pour $1 \leqslant i \leqslant n$) . Un tel point existe car il n'y a pas d'élément maximum dans $\mathfrak{N}$.

• Même chose si a_0 est plus petit que tous les a_i (pour $1 \leqslant i \leqslant n$) : on prend b_0 plus petit que tous les b_i (pour $1 \leqslant i \leqslant n$).

• Si a_0 est égal à l'un des a_i, disons a_k , on prend $b_0 = b_k$.

• Dans le cas restant, on choisit un indice $p \in \{1,2,\ldots,n\}$ tel que a_p soit le plus petit (au sens de l'ordre de $\mathfrak{M}$) des a_i (pour $1 \leqslant i \leqslant n$) plus grands que a_0 et et un indice $q \in \{1,2,\ldots,n\}$ tel que a_q soit le plus grand des a_i (pour $1 \leqslant i \leqslant n$) plus petits que

a_0. On a $a_q < a_0 < a_p$, et donc, $b_q < b_p$. On choisit alors b_0 dans N strictement compris entre b_q et b_p (ce qui est possible parce que l'ordre sur $\mathfrak{N}$ est dense).

On fait évidemment la même chose pour trouver a_0 connaissant b_0.

☺

LEMME 2 : *Soient* $\mathfrak{M}$ *et* $\mathfrak{N}$ *deux modèles de* T, $a_1,a_2,\ldots,a_n \in M$, $b_1,b_2,\ldots,b_n \in N$, *et on suppose que ces deux suites satisfont, respectivement dans* $\mathfrak{M}$ *et* $\mathfrak{N}$, *les mêmes formules atomiques ; alors, pour toute formule* $F[v_1,v_2,\ldots,v_n]$ *de* L,

(∗) $\mathfrak{M} \models F[a_1,a_2,\ldots,a_n]$ *si et seulement si* $\mathfrak{N} \models F[b_1,b_2,\ldots,b_n]$.

En admettant ce lemme, on conclut facilement que, si $\mathfrak{M}$ et $\mathfrak{N}$ sont deux modèles de T et si $\mathfrak{M}$ est une sous-structure de $\mathfrak{N}$, alors $\mathfrak{M} \prec \mathfrak{N}$: si $a_1,a_2,\ldots,a_n$ sont des points de M, alors les formules atomiques que cette suite satisfait dans $\mathfrak{M}$ sont les mêmes que celles qu'elle satisfait dans $\mathfrak{N}$ (parce que $\mathfrak{M}$ est une sous-structure de $\mathfrak{N}$). Les hypothèses du lemme sont donc vérifiées, et donc, pour toute formule $F[v_1,v_2,\ldots,v_n]$ de L,

$$\mathfrak{M} \models F[a_1,a_2,\ldots,a_n] \text{ si et seulement si } \mathfrak{N} \models F[a_1,a_2,\ldots,a_n] ;$$

autrement dit, $\mathfrak{M} \prec \mathfrak{N}$.

Il reste à démontrer le lemme 2.

☺ On suppose qu'aucun quantificateur universel n'apparaît dans F, ce que l'on peut toujours faire quitte à remplacer F par une formule équivalente (voir la remarque 3.10 du chapitre 3), et on démontre le lemme par induction sur F.

L'hypothèse du lemme dit que la condition (∗) est vérifiée si F est atomique. Il est immédiat que si (∗) est vérifiée pour les formules F_1 et F_2, elle l'est aussi pour les formules $\neg F_1$, $F_1 \wedge F_2$, $F_1 \vee F_2$, $F_1 \Rightarrow F_2$ et $F_1 \Longleftrightarrow F_2$. Reste le cas où $F[v_1,v_2,\ldots,v_n] = \exists v_0 G[v_0,v_1,\ldots,v_n]$; supposons (en plus du fait que les suites $(a_1,a_2,\ldots,a_n)$ et $(b_1,b_2,\ldots,b_n)$ satisfont respectivement dans $\mathfrak{M}$ et $\mathfrak{N}$ les mêmes formules atomiques) que :

$$\mathfrak{M} \models F[a_1,a_2,\ldots,a_n].$$

Il existe donc $a_0 \in M$ tel que :

$$\mathfrak{M} \models G[a_0,a_1,\ldots,a_n].$$

On choisit un élément b_0 dans N qui se situe par rapport aux b_i (pour $1 \leqslant i \leqslant n$) exactement comme a_0 se situe par rapport aux a_i, autrement dit tel que les suites $(a_0,a_1,\ldots,a_n)$ et $(b_0,b_1,\ldots,b_n)$ continuent de satisfaire les mêmes formules atomiques dans $\mathfrak{M}$ et $\mathfrak{N}$ respectivement (lemme 1). Puisque la formule G a un quantificateur de moins que la formule F, on peut lui appliquer l'hypothèse d'induction. On voit que :

$$\mathfrak{N} \models G[b_0,b_1,\ldots,b_n]$$

et donc que :

$$\mathfrak{N} \models F[b_1,b_2,\ldots,b_n].$$

On peut échanger les rôles de $\mathfrak{M}$ et de $\mathfrak{N}$, et montrer de la même façon que,

si $\mathfrak{N} \models F[b_1,b_2,\ldots,b_n]$, alors $\mathfrak{M} \models F[a_1,a_2,\ldots,a_n]$.

☺

Le test de Tarski-Vaught

1.4 Le résultat suivant, appelé **test de Tarski-Vaught**, est quelquefois pratique pour vérifier qu'une sous-structure est élémentaire :

THEOREME : *Soient* $\mathfrak{M}$ *une structure,* $\mathfrak{N}$ *une sous-structure de* $\mathfrak{M}$ *et supposons que, pour toute formule* $F[v_0,v_1,\ldots,v_n]$ *de* L *et tous éléments* $a_1,a_2,\ldots,a_n$ *dans* N, *si*

$$\mathfrak{M} \models \exists v_0 F[v_0,a_1,\ldots,a_n],$$

alors il existe a_0 *dans* N *tel que*

$$\mathfrak{M} \models F[a_0,a_1,\ldots,a_n].$$

Alors $\mathfrak{N} \prec \mathfrak{M}$.

La différence avec la définition 1.1 est que seule intervient la satisfaction des formules dans une des deux structures (la plus grande).

☺ On montre que pour toute formule $G[v_1,v_2,\ldots,v_n]$ et pour tous $a_1,a_2,\ldots,a_n$ de N,

$$\mathfrak{N} \models G[a_1,a_2,\ldots,a_n] \text{ si et seulement si } \mathfrak{M} \models G[a_1,a_2,\ldots,a_n].$$

Comme précédemment : on suppose qu'aucun quantificateur universel n'apparaît dans G (remarque 3.10 du chapitre 3) et on raisonne par induction sur G. Le cas des connecteurs propositionnels n'offre aucune difficulté. Considérons donc le cas où $G[v_1,v_2,\ldots,v_n] = \exists v_0 F[v_0,v_1,\ldots,v_n]$ (F a donc un quantificateur de moins que G).

- Si $\mathfrak{N} \models \exists v_0 F[v_0,a_1,a_2,\ldots,a_n]$, alors il existe $a_0 \in N$ tel que $\mathfrak{N} \models F[a_0,a_1,\ldots,a_n]$ et, par hypothèse d'induction, on voit que $\mathfrak{M} \models F[a_0,a_1,\ldots,a_n]$; par conséquent :

$$\mathfrak{M} \models \exists v_0 F[v_0,a_1,a_2,\ldots,a_n].$$

- Réciproquement, si $\mathfrak{M} \models \exists v_0 F[v_0,a_1,a_2,\ldots,a_n]$, alors, par l'hypothèse du théorème, il existe $a_0 \in N$ tel que $\mathfrak{M} \models F[a_0,a_1,\ldots,a_n]$. Par hypothèse d'induction, on obtient $\mathfrak{N} \models F[a_0,a_1,\ldots,a_n]$, et donc $\mathfrak{N} \models \exists v_0 F[v_0,a_1,a_2,\ldots,a_n]$.

☺

REMARQUE : En fait, il n'est même pas utile, pour pouvoir appliquer le test de Tarski-Vaught, de vérifier que $\mathfrak{N}$ est une sous-structure de $\mathfrak{M}$: supposons que A soit un sous-ensemble de M vérifiant : pour toute formule $F[v_0,v_1,\dots,v_n]$ de L et tous éléments $a_1,a_2,\dots,a_n$ dans A, si

$$\mathfrak{M} \models \exists v_0 F[v_0,a_1,\dots,a_n] ,$$

alors il existe a_0 dans A tel que

$$\mathfrak{M} \models F[a_0,a_1,\dots,a_n] ;$$

alors, A est clos pour les fonctions du langage : pour chaque symbole de fonction k-aire f, il suffit de considérer la formule $F = v_0 \simeq fv_1v_2\dots v_k$: autrement dit, A est une sous-structure de $\mathfrak{M}$ (A n'est pas vide puisque $\mathfrak{M} \models \exists v_0\, v_0 \simeq v_0$).

1.5 On va donner un exemple d'application du test de Tarski-Vaught. Auparavant, précisons que la cardinalité d'un langage L, notée card(L), est, par définition, égale à la cardinalité de l'ensemble des formules de L, donc égale à $\sup(\aleph_0,\mathrm{card}(X))$, si X désigne l'ensemble des symboles de constante, de fonction et de relation de L. La cardinalité d'une structure est naturellement la cardinalité de son ensemble de base. Le théorème suivant est connu sous le nom de **théorème de Löwenheim-Skolem descendant** :

THEOREME : *Soient* $\mathfrak{M}$ *une* L*-structure,* A *un sous-ensemble de* M*, et on suppose que* $\mathrm{card}(M) \geqslant \mathrm{card}(L)$*. Alors il existe une sous-structure élémentaire* $\mathfrak{M}_0$ *de* $\mathfrak{M}$ *contenant* A *et de cardinalité* $\sup(\mathrm{card}(A),\mathrm{card}(L))$.

☺ Quitte à agrandir l'ensemble A, on peut supposer que $\mathrm{card}(A) \geqslant \mathrm{card}(L)$. On remarque ensuite que, si B est un sous-ensemble de M et si $\mathrm{card}(B) \geqslant \mathrm{card}(L)$, alors la sous-structure de $\mathfrak{M}$ engendrée par B (c'est-à-dire le plus petit sous-ensemble N de M contenant B et clos pour les fonctions du langage) est de la même cardinalité que B (en effet, tout élément de N est l'interprétation d'un terme à paramètres dans B ; l'ensemble de ces termes est un ensemble de suites finies de $L \cup B$, et est donc de cardinalité inférieure ou égale à celle de B).

On définit par récurrence sur l'entier n des sous-ensembles $A_0 \subseteq A_1 \subseteq \dots \subseteq A_n \subseteq \dots$ de $\mathfrak{M}$ qui sont tous de cardinalité card(A) :

• A_0 est la sous-structure engendrée par A ;

• voici comment définir A_{i+1} à partir de A_i : pour chaque formule $F[v_0,v_1,\dots,v_n]$ de L et chaque suite $(a_1,a_2,\dots,a_n)$ de A_i, si $\mathfrak{M} \models \exists v_0 F[v_0,a_1,a_2,\dots,a_n]$, alors on choisit un point $c_{F,a_1,a_2,\dots,a_n}$ de M tel que $\mathfrak{M} \models F[c_{F,a_1,a_2,\dots,a_n},a_1,a_2,\dots,a_n]$; posons :

$$B_i = A_i \cup \{ c_{F,a_1,a_2,\dots,a_n} ;\ n \in \mathbb{N},\ F[v_0,v_1,\dots,v_n] \text{ est une formule de L, } a_1,a_2,\dots,a_n \text{ appartiennent à M et } \mathfrak{M} \models \exists v_0 F[v_0,a_1,a_2,\dots,a_n] \},$$

et appelons A_{i+1} la sous-structure de $\mathfrak{M}$ engendrée par B_i. Il y a card(L) formules F dans L et card(A_i) suites $(a_1,a_2,\ldots,a_n)$ dans A_i de longueur convenable. Il faut donc ajouter au plus card(A_i) points à A_i pour obtenir B_i, ce qui montre que card(A_{i+1}) = card(B_i) = card(A_i) = card(A).

On pose $\mathfrak{M}_0 = \bigcup_{i \in \mathbb{N}} A_i$. Il est clair que $\mathfrak{M}_0$ est une sous-structure de $\mathfrak{M}$ et que sa cardinalité est card(A) (voir le corollaire 4.14 du chapitre 7). On va maintenant utiliser le test de Tarski-Vaught pour montrer que c'est une sous-structure élémentaire.

En effet, soient $F[v_0,v_1,\ldots,v_n]$ une formule de L et $a_1,a_2,\ldots,a_n$ des points de M_0, et supposons que $\mathfrak{M} \models \exists v_0 F[v_0,a_1,a_2,\ldots,a_n]$. On sait qu'il existe un entier i tel que A_i contienne $a_1,a_2,\ldots,a_n$. Par construction de A_{i+1}, il existe dans cet ensemble, donc dans M_0, un point c tel que $\mathfrak{M} \models F[c,a_1,a_2,\ldots,a_n]$: c'est exactement l'hypothèse que réclame le test de Tarski-Vaught.

☺

2. CONSTRUCTIONS D'EXTENSIONS ELEMENTAIRES

Applications élémentaires

2.1 Voici encore une notion importante :

DEFINITION : *Soient* $\mathfrak{M}$ et $\mathfrak{N}$ *deux* L-*structures et* h *une application de* M *dans* N *; on dit que* h *est une* ***application élémentaire*** *si, pour toute formule* $F[v_1,v_2,\ldots,v_n]$ *de* L *et tous éléments* $a_1, a_2,\ldots,a_n$ *de* M, *on a* :

$$\mathfrak{M} \models F[a_1,a_2,\ldots,a_n] \text{ si et seulement si } \mathfrak{N} \models F[h(a_1),h(a_2),\ldots,h(a_n)].$$

On voit immédiatement, en considérant la formule $v_0 \simeq v_1$, qu'une application élémentaire est injective. Pour insister sur ce fait, on dira quelquefois **plongement élémentaire** au lieu d'application élémentaire. S'il existe une application élémentaire de $\mathfrak{M}$ dans $\mathfrak{N}$, on dira que **$\mathfrak{M}$ se plonge élémentairement dans $\mathfrak{N}$**. Il est aussi clair qu'une

application élémentaire est un monomorphisme de L-structures. La réciproque n'est pas vraie : pour s'en convaincre, il suffit de reprendre un exemple d'une sous-structure $\mathfrak{M}$ de $\mathfrak{N}$ qui n'est pas élémentaire (voir 1.1). L'application identité de M dans N est un monomorphisme qui n'est pas élémentaire. Cependant, on a :

2.2 PROPOSITION : *Soit* h *un monomorphisme d'une structure* $\mathfrak{M}$ *dans une structure* $\mathfrak{N}$. *Alors* h *est une application élémentaire si et seulement si l'image de* h *est une sous-structure élémentaire de* $\mathfrak{N}$.

☹ Soit $\mathfrak{N}_1$ l'image de h, ce qui fait que h induit un isomorphisme de $\mathfrak{M}$ sur $\mathfrak{N}_1$. On voit donc, par le théorème 5.2 du chapitre 3, que, pour toute formule $F[v_1,v_2,\ldots,v_n]$ de L et tous $a_1, a_2,\ldots,a_n$ de M, on a :

$$\mathfrak{M} \models F[a_1,a_2,\ldots,a_n] \text{ si et seulement si } \mathfrak{N}_1 \models F[h(a_1),h(a_2),\ldots,h(a_n)] .$$

• Supposons d'abord que $\mathfrak{N}_1 \prec \mathfrak{N}$. Alors :

$$\mathfrak{N}_1 \models F[h(a_1),h(a_2),\ldots,h(a_n)] \text{ si et seulement si } \mathfrak{N} \models F[h(a_1),h(a_2),\ldots,h(a_n)]$$

ce qui, avec l'équivalence ci-dessus, implique bien que h est élémentaire.

• Réciproquement, supposons que h soit élémentaire, et soient $b_1,b_2,\ldots,b_n$ des points de N_1. Il existe $a_1,a_2,\ldots,a_n$ dans M tels que $h(a_1) = b_1$, $h(a_2) = b_2,\ldots$, $h(a_n) = b_n$. Pour toute formule $F[v_1,v_2,\ldots,v_n]$ de L, on a :

$$\mathfrak{M} \models F[a_1,a_2,\ldots,a_n] \text{ si et seulement si } \mathfrak{N} \models F[h(a_1),h(a_2),\ldots,h(a_n)] ,$$

et donc :

$$\mathfrak{N} \models F[b_1,b_2,\ldots,b_n] \text{ si et seulement si } \mathfrak{N}_1 \models F[b_1,b_2,\ldots,b_n].$$

☺

COROLLAIRE : *S'il existe une application élémentaire de* $\mathfrak{M}$ *dans* $\mathfrak{N}$, *alors* $\mathfrak{M}$ *et* $\mathfrak{N}$ *sont élémentairement équivalents.*

☹ En effet, si $\mathfrak{N}_1$ est l'image de cette application élémentaire, $\mathfrak{N}_1 \equiv \mathfrak{N}$ parce que $\mathfrak{N}_1 \prec \mathfrak{N}$ et $\mathfrak{N}_1 \equiv \mathfrak{M}$ par isomorphisme.

☺

La méthode des diagrammes

2.3 On va maintenant exposer **la méthode des diagrammes** qui permet de construire des extensions et des extensions élémentaires. Cette méthode a d'ailleurs déjà été esquissée au chapitre 3 (5.10). Soit $\mathfrak{M}$ une L-structure ; on considère le langage L_M obtenu en ajoutant à L un symbole de constante $\underline{a}$ pour chaque élément $a \in M$. Alors $\mathfrak{M}$ s'enrichit naturellement en une L_M-structure que l'on notera $\mathfrak{M}^*$: il suffit d'interpréter $\underline{a}$ par a. Posons :

$$D(\mathfrak{M}) = \{ F[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n] ; F[v_1,v_2,\ldots,v_n] \text{ est une formule de L, } a_1,a_2,\ldots,a_n \in M \text{ et } \mathfrak{M} \models F[a_1,a_2,\ldots,a_n] \}.$$

On voit que $D(\mathfrak{M})$, que l'on appelle **le diagramme complet de** $\mathfrak{M}$, est la théorie complète de $\mathfrak{M}^*$. Ce qui est important, c'est que n'importe quel autre modèle de $D(\mathfrak{M})$, ou, plus exactement, le réduit au langage L de n'importe quel autre modèle de $D(\mathfrak{M})$, est, à isomorphisme près, une extension élémentaire de $\mathfrak{M}$. Expliquons-nous.

Soit $\mathfrak{N}^*$ une L_M-structure qui est un modèle de $D(\mathfrak{M})$. Notons $\mathfrak{N}$ le réduit de $\mathfrak{N}^*$ au langage L ($\mathfrak{N}$ est donc obtenu à partir de $\mathfrak{N}^*$ en oubliant les interprétations des symboles de constantes $\underline{a}$ pour $a \in M$). Pour chaque $a \in M$, appelons $g(a)$ l'interprétation de $\underline{a}$ dans $\mathfrak{N}^*$. On voit donc que g est une application de M dans N et que, pour toute formule $F[v_1,v_2,\ldots,v_n]$ de L et pour tous $a_1,a_2,\ldots,a_n$ dans M, on a :

(*) $\mathfrak{M} \models F[a_1,a_2,\ldots,a_n]$ si et seulement si $\mathfrak{N} \models F[g(a_1),g(a_2),\ldots,g(a_n)]$.

(Parce que ces deux conditions sont encore équivalentes à : $F[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n] \in D(\mathfrak{M})$, la première par définition de $D(\mathfrak{M})$, la seconde parce que $\mathfrak{N}^*$ est un modèle de $D(\mathfrak{M})$ et que les symboles $\underline{a}_i$ y sont interprétées par $g(a_i)$ et que $D(\mathfrak{M})$ est une théorie complète).

Autrement dit, g est une application élémentaire de $\mathfrak{M}$ dans $\mathfrak{N}$. On n'est donc pas très loin du but que l'on s'est fixé : $\mathfrak{N}$ n'est pas une extension élémentaire de $\mathfrak{M}$, mais seulement une extension élémentaire d'une structure isomorphe à $\mathfrak{M}$ (l'image de g). Pour réparer cette imperfection, on va montrer que l'on peut supposer que, pour tout $a \in M$, $g(a) = a$, et pour cela, on va faire une construction complètement formelle et totalement inintéressante. Elle fera l'objet du lemme suivant auquel on fera appel plusieurs fois au cours de cette section. Rappelons auparavant que le diagramme simple d'une structure $\mathfrak{M}$, noté $\Delta(\mathfrak{M})$, est la théorie suivante de L_M :

$$\Delta(\mathfrak{M}) = \{ H[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n] ; H[v_1,v_2,\ldots,v_n] \text{ est une formule sans quantificateur de L, } a_1,a_2,\ldots,a_n \text{ sont des points de } \mathfrak{M} \text{ et } \mathfrak{M} \models H[a_1,a_2,\ldots,a_n] \}.$$

(Voir chapitre 3, 5.10).

LEMME : *Si $\mathfrak{M}$ est une L-structure, alors tout modèle de $\Delta(\mathfrak{M})$ est isomorphe à une extension de $\mathfrak{M}^*$ (dans laquelle chaque symbole $\underline{a}$, pour $a \in M$, est donc interprété par a).*

☹ Soit $\mathfrak{N}$ un modèle de $\Delta(\mathfrak{M})$ et appelons g l'application de M dans N qui, à chaque $a \in M$, fait correspondre l'interprétation de $\underline{a}$ dans $\mathfrak{N}$. Prenons un ensemble M_1 contenant M et tel que $M_1 - M$ ait la même cardinalité que $N - g(M)$. On peut alors prolonger l'application g en une bijection g_1 de M_1 sur N. On définit une L_M-structure $\mathfrak{M}_1$ dont l'ensemble de base est M_1 en exigeant que g_1 soit un isomorphisme de $\mathfrak{M}_1$ dans $\mathfrak{N}$: tout d'abord, chacun des symboles $\underline{a}$, pour $a \in M$, est interprété par l'élément a ; ensuite, si R est un symbole de relation à p arguments, l'interprétation de R dans $\mathfrak{M}_1$ est :

$$\{(a_1,a_2,...,a_p) \in M_1^p \ ; \ \mathfrak{N} \models Rg_1(a_1)g_1(a_2)...g_1(a_p)\}.$$

Les interprétations des symboles de constante et de fonction sont définies de façon analogue. Il est bien clair que la structure $\mathfrak{M}_1$ ainsi définie est une extension de $\mathfrak{M}^*$.

☺

Si, comme on le supposait plus haut, $\mathfrak{N}$ est un modèle de $D(\mathfrak{M})$ (et pas seulement de $\Delta(\mathfrak{M})$), alors $\mathfrak{M}$ est une sous-structure élémentaire du réduit de $\mathfrak{M}_1$ à L : soit $F[v_1,v_2,...,v_n]$ une formule de L et soient $a_1,a_2,...,a_n$ des points de M. On a :

$\mathfrak{M}_1 \models F[a_1,a_2,...,a_n]$ si et seulement si $\mathfrak{N} \models F[g_1(a_1),g_1(a_2),...,g_1(a_n)]$ (parce que g_1 est un isomorphisme),

si et seulement si

$\mathfrak{N} \models F[g(a_1),g(a_2),...,g(a_n)]$ (parce que g_1 prolonge g),

si et seulement si

$\mathfrak{M} \models F[a_1,a_2,...,a_n]$ par la condition (*).

2.4 Voici un premier exemple d'application de cette technique :

THEOREME : *Toute structure infinie $\mathfrak{M}$ admet une extension élémentaire propre (c'est-à-dire une extention élémentaire différente de $\mathfrak{M}$ elle-même).*

☹ Ajoutons encore à L_M un nouveau symbole de constante c et considérons la théorie suivante T' dans le langage ainsi obtenu :

$$T' = D(\mathfrak{M}) \cup \{\neg c \simeq \underline{a} \ ; \ a \in M\}.$$

On voit tout d'abord, par le théorème de compacité, que cette théorie a un modèle : en effet tout sous-ensemble fini de T' est inclus dans un ensemble de la forme $D(\mathfrak{M}) \cup \{\neg c \simeq \underline{a} \ ; \ a \in A\}$ où A est un sous-ensemble fini de M. Pour en avoir un modèle, il suffit d'enrichir $\mathfrak{M}^*$ en interprétant c par un point de M n'appartenant pas à A (ce qui est possible puisque M est infini alors que A est fini).

Soit $\mathfrak{N}^*$ un modèle de T' et $\mathfrak{N}$ son réduit au langage L ; on a vu que l'on peut supposer que $\mathfrak{N}$ est une extension élémentaire de $\mathfrak{M}$. Il est bien clair que l'interprétation du symbole c dans $\mathfrak{N}^*$ ne peut pas appartenir à M, ce qui montre que $\mathfrak{N} \neq \mathfrak{M}$.

☺

Pour alléger les notations, lorsque l'on appliquera cette méthode, on se dispensera de distinguer les structures $\mathfrak{M}$ et $\mathfrak{M}^*$. Il s'agit évidemment d'un abus de langage, mais qui ne présente pas de danger.

2.5 La même idée appliquée de façon plus audacieuse donne le **théorème de Lowenheim-Skolem ascendant** :

THEOREME : *Soient $\mathfrak{M}$ une L-structure* infinie *et κ un cardinal tel que $\kappa \geqslant \sup(\mathrm{card}(M), \mathrm{card}(L))$. Alors il existe une extension élémentaire $\mathfrak{N}$ de $\mathfrak{M}$ de cardinalité κ.*

☹ Il suffit en fait de construire $\mathfrak{N} \succ \mathfrak{M}$, avec $\mathrm{card}(N) \geqslant \kappa$. Si on a fait cela, on choisit un sous-ensemble A de N contenant M et de cardinalité κ, et, par le théorème de Lowenheim-Skolem descendant (théorème 1.5), on construit $\mathfrak{N}_0$ telle que $M \subseteq N_0$, $\mathfrak{N}_0 \prec \mathfrak{N}$ et $\mathrm{card}(N_0) = \kappa$. On a déjà remarqué (remarque 1.2) que cela implique $\mathfrak{M} \prec \mathfrak{N}_0$.

Introduisons, pour chaque $i \in \kappa$ un nouveau symbole de constante c_i et considérons la théorie suivante :

$$T' = D(\mathfrak{M}) \cup \{\neg c_i \simeq c_j \,;\, i \in \kappa, j \in \kappa \text{ et } i \neq j\}.$$

Cette théorie est consistante : tout sous-ensemble fini de T' est inclus dans un ensemble de la forme $D(\mathfrak{M}) \cup \{\neg c_i \simeq c_j \,;\, i,j \in A \text{ et } i \neq j\}$ où A est un sous-ensemble fini de κ, et pour en avoir un modèle, il suffit d'interpréter les c_i, pour $i \in A$, par des points de M deux à deux distincts, ce qui est possible puisque M est infini.

On termine la preuve comme précédemment : soit $\mathfrak{N}$ un modèle de T', et on peut supposer que $\mathfrak{N} \succ \mathfrak{M}$. Alors les c_i, pour $i \in \kappa$, sont interprétés dans $\mathfrak{N}$ par des points distincts, ce qui oblige la cardinalité de N à être au moins κ.

☺

Des deux théorèmes de Lowenheim-Skolem découle immédiatement :

COROLLAIRE : *Soient T une théorie dans un langage L et κ un cardinal supérieur ou égal à $\mathrm{card}(L)$. Si T a un modèle infini, alors T a un modèle de cardinalité κ.*

2.6 Pour le prochain théorème, qui est généralement appelé **théorème de Vaught**, nous avons besoin de la définition suivante :

DEFINITION : *Soient* T *une théorie et* κ *un cardinal. On dit que* T *est* ***κ-catégorique*** *si, premièrement,* T *admet un modèle de cardinalité* κ *et, deuxièmement, tous les modèles de cardinalité* κ *sont isomorphes.*

THEOREME : *Soit* T *une théorie dans un langage* L *n'ayant pas de modèle fini. Supposons que* T *soit* κ*-catégorique, pour un cardinal* κ *supérieur ou égal à* card(L). *Alors* T *est complète.*

☹ On suppose le contraire ; il existe donc dans L une formule close F telle que $T_1 = T \cup \{F\}$ et $T_2 = T \cup \{\neg F\}$ soient toutes les deux consistantes. D'après le théorème de Lowenheim-Skolem ascendant, on voit qu'il existe des modèles $\mathfrak{M}_1$ de T_1 et $\mathfrak{M}_2$ de T_2 de cardinalité κ ; $\mathfrak{M}_1$ et $\mathfrak{M}_2$ ne peuvent pas être isomorphes, ce qui contredit la κ-catégoricité.
☺

2.7 EXEMPLE : Les ordres denses sans extrémités.

Reprenons la théorie T des ordres denses sans extrémités dont les axiomes sont présentés en 1.3. Il est clair que cette théorie n'admet pas de modèle fini. On va voir qu'elle est $\aleph_0$-catégorique, ce qui, avec le théorème de Vaught, impliquera qu'elle est complète.

Soient $\mathfrak{M}$ et $\mathfrak{N}$ deux modèles dénombrables de T ; établissons un isomorphisme par un « **va et vient** » entre ces deux structures. On utilise d'abord l'hypothèse que M et N sont dénombrables : on peut donc trouver des énumérations de ces deux ensembles :

$$M = \{m_i \,;\, i \in \mathbb{N}\} \text{ et } N = \{n_i \,;\, i \in \mathbb{N}\}.$$

On définit par récurrence deux suites $(a_p \,;\, p \in \mathbb{N})$ et $(b_p \,;\, p \in \mathbb{N})$ telle que, pour tout entier p, $a_p \in M$, $b_p \in N$ et les suites $(a_0,a_1,\ldots,a_{p-1})$ et $(b_0,b_1,\ldots,b_{p-1})$ satisfont les respectivement dans $\mathfrak{M}$ et $\mathfrak{N}$ les mêmes formules atomiques. Pour définir a_p et b_p, on distingue deux cas :

• si p est pair, disons $p = 2i$, on pose $a_p = m_i$; avec le lemme 1 de 1.3, on voit qu'il existe un point de N, que l'on appelle b_p tel que les suites $(a_0,a_1,\ldots,a_p)$ et $(b_0,b_1,\ldots,b_p)$ satisfont encore les mêmes formules atomiques dans $\mathfrak{M}$ et $\mathfrak{N}$ respectivement.

• Si p est impair, par exemple $p = 2i + 1$, on pose $b_p = n_i$, et on choisit a_p dans M de sorte que $(a_0,a_1,\ldots,a_p)$ et $(b_0,b_1,\ldots,b_p)$ satisfont les mêmes formules atomiques dans $\mathfrak{M}$ et $\mathfrak{N}$ respectivement.

On suppose par exemple que $q \leqslant p$ et on remarque que $a_p = a_q$ si et seulement si $b_p = b_q$ (parce que $(a_0,a_1,\ldots,a_p)$ et $(b_0,b_1,\ldots,b_p)$ satisfont les mêmes formules atomiques). On peut donc définir une application f de $\{a_k \,;\, k \in \mathbb{N}\}$ dans $\{b_k \,;\, k \in \mathbb{N}\}$ en posant : pour

tout entier k, $f(a_k) = b_k$. Par choix des a_p pour p pair, on voit que $\{a_k ; k \in \mathbb{N}\} = M$, et le choix de b_p pour p impair nous assure que $\{b_k ; k \in \mathbb{N}\} = N$; f est donc une bijection de M dans N, et c'est un isomorphisme de $\mathfrak{M}$ dans $\mathfrak{N}$ parce que, pour tout p, les suites $(a_0,a_1,\ldots,a_p)$ et $(b_0,b_1,\ldots,b_p)$ satisfont les mêmes formules atomiques.

2.8 EXEMPLE : **les groupes abéliens divisibles sans torsion.**

Dans le langage des groupes $\{0,+\}$, on considère la théorie suivante :

(i) $\forall v_0 \forall v_1 \forall v_2 \, (v_0 + v_1) + v_2 \simeq v_0 + (v_1 + v_2)$

(ii) $\forall v_0 \forall v_1 \, v_0 + v_1 \simeq v_1 + v_0$

(iii) $\forall v_0 \, v_0 + 0 \simeq v_0$

(iv) $\forall v_0 \exists v_1 \, v_0 + v_1 \simeq 0$.

(v) $\exists v_0 \, (\neg v_0 \simeq 0)$

(vi) $\forall v_0 (n \cdot v_0 \simeq 0 \Longrightarrow v_0 \simeq 0)$ pour chaque entier n strictement positif, où $n \cdot v$ désigne le terme $((\ldots(v + v) + v)\ldots) + v)$ avec n occurences du symbole v.

(vii) $\forall v_0 \exists v_1 \, v_0 \simeq n \cdot v_1$ pour tout $n \in \mathbb{N}$, $n \neq 0$.

On a là une théorie infinie (à cause de (vi) et (vii) qui sont en fait des schémas d'axiomes). Les axiomes (i)-(iv) expriment que l'on a affaire à un groupe abélien, l'axiome (v) dit que ce groupe n'est pas trivial, les axiomes (vi) que ce groupe est **sans torsion** et les axiomes (vii) que ce groupe est **divisible**. On va montrer que cette théorie est complète en utilisant le théorème de Vaught.

Le groupe $<\mathbb{Q},0,+>$ est un modèle de T, ce qui montre que T est consistante. Mais T a d'autres modèles : soit V un $\mathbb{Q}$-espace vectoriel dont $\times$ est la multiplication scalaire. Alors, le groupe G sous-jacent à V est un groupe abélien divisible sans torsion : en effet si $p \in \mathbb{N}$ et $a \in V$,

$$p \times a = (1 + 1 + \cdots + 1) \times a = 1 \times a + 1 \times a + \cdots + 1 \times a = a + a + a + \cdots + a = p \cdot a$$

et si $p \cdot a = 0$ avec $p \neq 0$, alors $0 = p^{-1} \times (p \cdot a) = p^{-1} \times (p \times a) = a$, ce qui montre que G est sans torsion. Pour la divisibilité, on a bien $p \cdot (p^{-1} \times a) = a$.

En fait, il y a une correspondance bijective entre les $\mathbb{Q}$-espaces vectoriels et les groupes abéliens divisibles sans torsion : si V est un espace vectoriel sur $\mathbb{Q}$, on vient de voir que son groupe sous-jacent que l'on notera V^- est un groupe abélien divisible sans torsion ; réciproquement, si G un groupe abélien divisible sans torsion, alors il existe un unique $\mathbb{Q}$-espace vectoriel, que l'on appellera G^+ dont le groupe sous-jacent est G, c'est-à-dire tel que $(G^+)^- = G$: si $a \in G$ et $r = p/q$ ($p \in \mathbb{N}$, $q \in \mathbb{N}^*$), $r \times a$ doit être l'élément x de G, qui est unique, tel que $q \cdot x = p \cdot a$, et si r est négatif, il faut que $r \times a$ soit égal à $-((-r) \times a)$. On voit de plus que si G et G' sont deux groupes abéliens divisibles sans torsion, une application h de G dans G' est un isomorphisme de groupes si et seulement si c'est un isomorphisme de $\mathbb{Q}$-espaces vectoriels de G^+ dans G'^+.

Cela montre en particulier que T n'est pas $\aleph_0$-catégorique : les $\mathbb{Q}$-espaces vectoriels de dimension deux et trois par exemple sont dénombrables, et donnent naissance à des modèles de T qui ne sont pas isomorphes.

Pour montrer que T est $\aleph_1$-catégorique (en fait : que T est λ-catégorique pour n'importe quel cardinal non dénombrable λ), il suffit de voir que deux $\mathbb{Q}$-espaces vectoriels de cardinalité $\aleph_1$ sont nécessairement isomorphes (parce qu'ils doivent avoir des bases de cardinalité $\aleph_1$; c'est un petit exercice sur les cardinalités).

Une remarque encore : il y a des théories complètes qui n'ont que des modèles infinis et qui ne sont catégoriques en aucun cardinal infini (voir exercices 4, 6 et 11).

2.9 Voici, pour terminer cette section, un procédé de construction de L-structures qui, avec les bonnes hypothèses, donne des extensions élémentaires. Soient $(I,<)$ un ensemble totalement ordonné et, pour chaque $i \in I$, $\mathfrak{M}_i$ une L-structure ; on suppose que si $i < j$, alors $\mathfrak{M}_i$ est une sous-structure de $\mathfrak{M}_j$. Posons $M = \bigcup_{i \in I} M_i$. On peut facilement (et de façon unique) construire une L-structure $\mathfrak{M}$, que l'on notera $\bigcup_{i \in I} \mathfrak{M}_i$, dont l'ensemble de base est M, de telle sorte que toutes les structures $\mathfrak{M}_i$ soient des sous-structures de $\mathfrak{M}$. Par exemple, si R est un symbole de relation d'arité p, et si $a_1,a_2,\ldots,a_p$ sont des points de M, on choisit un indice $i \in I$ tel que les points $a_1,a_2,\ldots,a_p$ appartiennent tous à M_i (ce qui est possible puisque les ensembles M_i sont totalement ordonnés par inclusion), et on décide que $(a_1,a_2,\ldots,a_p) \in \overline{R}^{\mathfrak{M}}$ si et seulement si $(a_1,a_2,\ldots,a_p) \in \overline{R}^{\mathfrak{M}_i}$. Cette décision ne dépend pas du choix de l'indice i : si j est aussi tel que $(a_1,a_2,\ldots,a_p) \in M_j$, alors on a soit $i \leqslant j$, soit $j < i$. Donc, soit $\mathfrak{M}_i$ est sous-structure de $\mathfrak{M}_j$, soit $\mathfrak{M}_j$ est sous-structure de $\mathfrak{M}_i$. Dans les deux cas, $(a_1,a_2,\ldots,a_p) \in \overline{R}^{\mathfrak{M}_i}$ si et seulement si $(a_1,a_2,\ldots,a_p) \in \overline{R}^{\mathfrak{M}_j}$. On définit de même les interprétations des symboles de constante et des symboles de fonction.

On en vient maintenant à un théorème fort utile, connu sous le nom de **théorème de l'union de chaîne de Tarski** :

THEOREME : *Soient* $(I,<)$ *un ensemble totalement ordonné, et pour chaque* $i \in I$, $\mathfrak{M}_i$ *une* L-*structure ; on suppose que, si* $i < j$, *alors* $\mathfrak{M}_i \prec \mathfrak{M}_j$. *Posons* $\mathfrak{M} = \bigcup_{i \in I} \mathfrak{M}_i$. *Alors pour tout* $j \in I$, $\mathfrak{M}_j$ *est une sous-structure élémentaire de* $\mathfrak{M}$.

☺ On montre par induction sur la formule $F[v_1,v_2,\ldots,v_p]$ que, pour tout $i \in I$ et tous $a_1,a_2,\ldots,a_p \in M_i$,

$$\mathfrak{M} \models F[a_1,a_2,\ldots,a_p] \text{ si et seulement si } \mathfrak{M}_i \models F[a_1,a_2,\ldots,a_p].$$

Comme on l'a plusieurs fois remarqué, on peut supposer que le quantificateur universel n'a pas d'occurrence dans F.

Il n'y a pas de problème pour les formules atomiques : $\mathfrak{M}_i$ est une sous-structure de $\mathfrak{M}$. Le cas des connecteurs propositionnels est évident. Supposons donc que $F = \exists v_0 G[v_0,v_1,\ldots,v_n]$, et soient $i \in I$ et $a_1,a_2,\ldots,a_p \in M_i$.

• Si $\mathfrak{M}_i \models \exists v_0 G[v_0,a_1,a_2,\ldots,a_p]$, alors il existe un point a_0 de M_i tel que $\mathfrak{M}_i \models G[a_0,a_1,\ldots,a_p]$; on voit par hypothèse d'induction que $\mathfrak{M} \models G[a_0,a_1,\ldots,a_p]$, et donc que $\mathfrak{M} \models F[a_1,a_2,\ldots,a_p]$.

• Si $\mathfrak{M} \models \exists v_0 G[v_0,a_1,a_2,\ldots,a_p]$, alors il existe un point a_0 de M tel que $\mathfrak{M} \models G[a_0,a_1,\ldots,a_p]$; il existe donc $j \in I$, $j > i$ tel que $a_0 \in M_j$, et, par hypothèse d'induction, $\mathfrak{M}_j \models G[a_0,a_1,\ldots,a_p]$ et donc $\mathfrak{M}_j \models \exists v_0 G[v_0,a_1,a_2,\ldots,a_p]$; mais puisque $\mathfrak{M}_i \prec \mathfrak{M}_j$, on a aussi $\mathfrak{M}_i \models F[a_1,a_2,\ldots,a_p]$.

☺

3. LES THEOREMES D'INTERPOLATION ET DE DEFINISSABILITE

3.1 On a vu au début de la section précédente que, s'il existe une application élémentaire entre deux structures, alors celles-ci sont élémentairement équivalentes. La réciproque est fausse (voir exercice 4). On a cependant :

THEOREME : *Soient $\mathfrak{M}_1$ et $\mathfrak{M}_2$ deux L-structures. Alors $\mathfrak{M}_1$ et $\mathfrak{M}_2$ sont élémentairement équivalentes si et seulement si elles se plongent élémentairement toutes les deux dans une même troisième.*

☺ Un sens est clair : si $\mathfrak{M}_1$ et $\mathfrak{M}_2$ se plongent élémentairement toutes les deux dans $\mathfrak{M}_3$, on a bien : $\mathfrak{M}_1 \equiv \mathfrak{M}_3 \equiv \mathfrak{M}_2$.

Réciproquement, supposons que $\mathfrak{M}_1$ et $\mathfrak{M}_2$ soient élémentairement équivalentes. On va utiliser la méthodes des diagrammes. On considère le langage L' obtenu en ajoutant à L : pour chaque élément a de M_1 un nouveau symbole de constante $\underline{a}$ et pour

chaque élément b de M_2 un nouveau symbole de constante $\bar{b}$. Attention : tous ces symboles doivent être différents et, en particulier, si a appartient à la fois à M_1 et M_2, il faut prendre bien soin de choisir $\underline{a}$ différent de $\bar{a}$.

Introduisons les diagrammes :

$D(\mathfrak{M}_1) = \{ F[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n] ; F[v_1,v_2,\ldots,v_n]$ est une formule de L,

$a_1,a_2,\ldots,a_n \in M_1$, et $\mathfrak{M}_1 \models F[a_1,a_2,\ldots,a_n] \}$

et $D(\mathfrak{M}_2) = \{ F[\bar{b}_1,\bar{b}_2,\ldots,\bar{b}_n] ; F[v_1,v_2,\ldots,v_n]$ est une formule de L,

$b_1,b_2,\ldots,b_n \in M_2$, et $\mathfrak{M}_2 \models F[b_1,b_2,\ldots,b_n] \}$.

On a vu que $\mathfrak{M}_1$ se plonge élémentairement dans tout modèle de $D(\mathfrak{M}_1)$, et de même, $\mathfrak{M}_2$ se plonge élémentairement dans tout modèle de $D(\mathfrak{M}_1)$. Il suffit donc de montrer que $T' = D(\mathfrak{M}_1) \cup D(\mathfrak{M}_2)$ est une théorie consistante. On utilise pour cela le théorème de compacité. Remarquons que $D(\mathfrak{M}_1)$ est clos par conjonction. Donc un sous-ensemble fini de $D(\mathfrak{M}_1)$ est équivalent à une formule $F[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n]$ de $D(\mathfrak{M}_1)$ et, si T' était contradictoire, il existerait une telle formule telle que :

$$D(\mathfrak{M}_2) \vdash \neg F[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n].$$

Mais comme les $\underline{a}_i$ n'apparaissent pas dans $D(\mathfrak{M}_2)$, on a (voir chapitre 4, lemme 2.4) :

$$D(\mathfrak{M}_2) \vdash \forall v_1 \forall v_2 \ldots \forall v_n \neg F[v_1,v_2,\ldots,v_n].$$

Donc $\forall v_1 \forall v_2 \ldots \forall v_n \neg F[v_1,v_2,\ldots,v_n]$ est une formule close de L qui est vraie dans $\mathfrak{M}_2$, qui doit par conséquent être vraie dans $\mathfrak{M}_1$, ce qui est contradictoire avec $\mathfrak{M}_1 \models F[a_1,a_2,\ldots,a_n]$.
☺

3.2 Le **lemme de consistance de Robinson**, qui est le théorème qui suit, fournit un très bel exemple de construction de modèle.

THEOREME : *Soient* T *une théorie complète dans un langage* L, L_1 *et* L_2 *deux enrichissements de* L *tels que* $L_1 \cap L_2 = L$, *et* T_1 *et* T_2 *deux théories consistantes dans les langages* L_1 *et* L_2 *respectivement, contenant toutes les deux* T. *Alors* $T_1 \cup T_2$ *est consistante.*

☹ La preuve se fait au moyen des trois lemmes qui vont suivre. Auparavant, fixons une notation : si $\mathfrak{M}$ est une L_1- ou une L_2-structure, $\mathfrak{M}^-$ désignera le réduit de $\mathfrak{M}$ à L.

LEMME 1 : *Soit* $\mathfrak{M}$ *un modèle de* T. *Alors il existe un modèle* $\mathfrak{B}$ *de* T_2 *tel que* $\mathfrak{M} \prec \mathfrak{B}^-$.

☹ Par la méthode des diagrammes : il sufffit de montrer que $T_2 \cup D(\mathfrak{M})$ est consistante. Si on suppose le contraire dans le but d'obtenir une contradiction, et en utilisant le théorème de compacité et le fait que $D(\mathfrak{M})$ est clos par conjonction, on obtient une formule $F[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n]$ de $D(\mathfrak{M})$ telle que $T_2 \vdash \neg F[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n]$. Les symboles $\underline{a}_i$ ne font pas partie du langage L_2 dans lequel est exprimée T_2. Par conséquent :

$$T_2 \vdash \forall v_1 \forall v_2 \ldots \forall v_n \neg F[v_1,v_2,\ldots,v_n].$$

La formule $\forall v_1 \forall v_2 \ldots \forall v_n \neg F[v_1,v_2,\ldots,v_n]$ est dans L, et T est contenue dans T_2 ; on voit donc que $\neg \forall v_1 \forall v_2 \ldots \forall v_n \neg F[v_1,v_2,\ldots,v_n]$ ne peut pas être conséquence de T ; puisque T est complète, $\forall v_1 \forall v_2 \ldots \forall v_n \neg F[v_1,v_2,\ldots,v_n]$ est conséquence de T. On obtient une contradiction puisque $\mathfrak{M}$ est un modèle de T et que $\mathfrak{M} \models F[a_1,a_2,\ldots,a_n]$.

☺

LEMME 2 : *Soient $\mathfrak{A}_1$ un modèle de T_1, $\mathfrak{M}$ un modèle de T, et on suppose que $\mathfrak{A}_1^- \prec \mathfrak{M}$. Alors il existe une L_1-structure $\mathfrak{A}_2$ tel que $\mathfrak{A}_1 \prec \mathfrak{A}_2$ et $\mathfrak{M} \prec \mathfrak{A}_2^-$ (et donc $\mathfrak{A}_2$ est un modèle de T_1).*

☹ On utilise toujours la même méthode : il suffit de construire un modèle de $T' = D(\mathfrak{M}) \cup D(\mathfrak{M}_1)$, où, rappelons-le,

$D(\mathfrak{M}) = \{ F[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n]$; $F[v_1,v_2,\ldots,v_n]$ est une formule de L, $a_1,a_2,\ldots,a_n \in M$, et $\mathfrak{M} \models F[a_1,a_2,\ldots,a_n] \}$

et $D(\mathfrak{A}_1) = \{ F[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n]$; $F[v_1,v_2,\ldots,v_n]$ est une formule de L_1, $a_1,a_2,\ldots,a_n \in A_1$, et $\mathfrak{A}_1 \models F[a_1,a_2,\ldots,a_n] \}$.

Il faut insister sur le fait que T' est une théorie dans $L_1(M)$. Contrairement à ce qu'on a fait pour le théorème 3.1, on n'introduit qu'un seul symbole de constante $\underline{a}$ pour chaque élément a de A_1 (l'ensemble de base de $\mathfrak{A}_1$) qui sert à la fois dans $D(\mathfrak{M})$ et dans $D(\mathfrak{A}_1)$; c'est grâce à cela que l'on pourra considérer un modèle de T' comme une extension élémentaire de $\mathfrak{A}_1$ et son L-réduit comme une extension élémentaire de $\mathfrak{M}$.

On raisonne encore par l'absurde ; on suppose que T' n'est pas consistante, et on en déduit une formule de $D(\mathfrak{M})$ contradictoire avec $D(\mathfrak{A}_1)$. On peut écrire cette formule sous la forme $F[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n,\underline{a}_{n+1},\ldots,\underline{a}_{n+p}]$ où F est une formule de L, $a_1,a_2,\ldots,a_n \in A_1$ et $a_{n+1},a_{n+2},\ldots, a_{n+p} \in M - A_1$.

Comme $D(\mathfrak{A}_1) \vdash \neg F[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n,\underline{a}_{n+1},\ldots,\underline{a}_{n+p}]$ et que les $\underline{a}_i$, pour i compris entre $n+1$ et $n+p$, n'apparaissent pas dans $D(\mathfrak{A}_1)$, on en déduit que :

$$D(\mathfrak{A}_1) \vdash \forall v_1 \forall v_2 \ldots \forall v_p \neg F[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n,v_1,\ldots,v_p], \text{ donc que}$$

$$\mathfrak{A}_1 \models \forall v_1 \forall v_2 \ldots \forall v_p \neg F[a_1,a_2,\ldots,a_n,v_1,\ldots,v_p].$$

Il est clair que $\mathfrak{M} \models \exists v_1 \exists v_2 \ldots \exists v_p F[a_1,a_2,\ldots,a_n,v_1,\ldots,v_p]$, et ceci contredit le fait que $\mathfrak{A}_1^- \prec \mathfrak{M}$.

☺

Evidemment, on peut remplacer T_1 par T_2 :

LEMME 2 bis : *Soient* $\mathfrak{B}_1$ *un modèle de* T_2, $\mathfrak{M}$ *un modèle de* T, *et on suppose que* $\mathfrak{B}_1^- \prec \mathfrak{M}$. *Alors il existe un modèle* $\mathfrak{B}_2$ *de* T_2 *tel que* $\mathfrak{B}_1 \prec \mathfrak{B}_2$ *et* $\mathfrak{M} \prec \mathfrak{B}_2^-$.

On peut maintenant terminer la preuve du lemme de consistance en construisant un modèle de $T_1 \cup T_2$. On part d'un modèle $\mathfrak{A}_1$ de T_1 ; $\mathfrak{A}_1^-$ est un modèle de T. On peut donc appliquer le lemme 1 et on trouve un modèle $\mathfrak{B}_1$ de T_2 tel que $\mathfrak{A}_1^- \prec \mathfrak{B}_1^-$. Ensuite, on applique le lemme 2 et on trouve un modèle $\mathfrak{A}_2$ de T_1 tel que $\mathfrak{A}_1 \prec \mathfrak{A}_2$ et $\mathfrak{B}_1^- \prec \mathfrak{A}_2^-$. On applique ensuite alternativement les lemmes 2 bis et 2 et on trouve des structures $\mathfrak{A}_n$, modèles de T_1 et $\mathfrak{B}_n$, modèles de T_2, telles que, pour tour entier n :

$$\mathfrak{A}_n \prec \mathfrak{A}_{n+1} \ , \ \mathfrak{B}_n \prec \mathfrak{B}_{n+1} \ , \mathfrak{A}_n^- \prec \mathfrak{B}_n^- \text{ et } \mathfrak{B}_n^- \prec \mathfrak{A}_{n+1}^- .$$

D'après le théorème de l'union de chaîne, $\mathfrak{A} = \bigcup_{n \geqslant 1} \mathfrak{A}_n$ est une extension élémentaire de $\mathfrak{A}_1$, donc un modèle de T_1, et de même, $\mathfrak{B} = \bigcup_{n \geqslant 1} \mathfrak{B}_n$ est un modèle de T_2. Or ces deux structures ont même ensemble de base, à savoir $\bigcup_{n \geqslant 1} A_n = \bigcup_{n \geqslant 1} B_n$, et même L-réduit, à savoir $\bigcup_{n \geqslant 1} \mathfrak{A}_n^- = \bigcup_{n \geqslant 1} \mathfrak{B}_n^-$. On obtient donc un modèle de $T_1 \cup T_2$ en considérant la $(L_1 \cup L_2)$-structure dont la L_1-restriction est $\mathfrak{A}$ et la L_2-restriction est $\mathfrak{B}$ (c'est ici qu'intervient l'hypothèse $L_1 \cap L_2 = L$: elle permet d'interpréter sans ambiguïté les symboles de $L_1 \cup L_2$ qui ne sont pas dans L).
☺

3.3 On comparera le théorème suivant, appelé le **théorème d'interpolation de Craig**, et qui est une conséquence du lemme de consistance de Robinson, avec le théorème 4.2 du chapitre 1.

THEOREME : *Soient* F *et* G *deux formules closes et on suppose que* $\vdash F \Longrightarrow G$ *est universellement valide. Alors il existe une formule* H *telle que :*

1) $\vdash F \Longrightarrow H$;

2) $\vdash H \Longrightarrow G$;

3) tous les symboles de constante, de fonction ou de prédicat (à l'exception de l'égalité) apparaissant dans H *apparaissent à la fois dans* F *et dans* G.

Une formule satisfaisant les conditions 1), 2) et 3) est appelée une ***interpolante entre*** F ***et*** G.

On remarque que l'on peut donner à ce théorème un sens purement syntaxique, où seule la déduction formelle intervient et où il n'est absolument pas question de modèle. Il en existe des preuves purement syntaxiques, mais ce n'est pas le cas de celle qui suit.

⊖ Soit L le langage composé de l'égalité et des symboles communs à F et G. Il s'agit de trouver une formule close de L telle que $\vdash (F \Rightarrow H) \wedge (H \Rightarrow G)$. On va supposer que c'est impossible et en déduire une contradiction. L'idée est de construire une théorie complète T dans L telle que $T \cup \{F\}$ et $T \cup \{\neg G\}$ soient toutes deux consistantes. Le lemme de consistance de Robinson nous dira alors que $T \cup \{F, \neg G\}$ est consistant, ce qui est absurde puisque $\vdash F \Rightarrow G$.

Le langage L est dénombrable. On peut donc trouver une énumération $\{J_n \,;\, n \in \mathbb{N}\}$ de toutes les formules closes de L, et on suppose que $J_0 = \exists v_0(v_0 \simeq v_0)$. On construit alors par récurrence sur l'entier n une suite de formules $(K_n \,;\, n \in \mathbb{N})$ de L de telle sorte que, pour tout $n \in \mathbb{N}$:

i) $\vdash K_{n+1} \Rightarrow K_n$;

ii) $\vdash K_n \Rightarrow J_n$ ou bien $\vdash K_n \Rightarrow \neg J_n$;

iii) les formules $F \wedge K_n$ et $G \wedge K_n$ n'admettent pas d'interpolante.

On démarre avec $K_0 = \exists v_0(v_0 \simeq v_0)$. Les conditions et ii) sont triviales et c'est parce qu'on a supposé que F et G n'admettaient pas d'interpolante que iii) est vérifiée. Construisons maintenant K_{n+1} à partir de K_n .

La remarque cruciale, c'est que l'une au moins des deux éventualités suivantes se produit :

- $F \wedge K_n \wedge J_{n+1}$ et $G \wedge K_n \wedge J_{n+1}$ n'ont pas d'interpolante.
- $F \wedge K_n \wedge \neg J_{n+1}$ et $G \wedge K_n \wedge \neg J_{n+1}$ n'ont pas d'interpolante.

En effet, si on suppose le contraire, il existe des formules closes de L, H_0 et H_1, telles que :

$$\vdash (F \wedge K_n \wedge J_{n+1}) \Rightarrow H_0\,, \qquad \vdash H_0 \Rightarrow (G \wedge K_n \wedge J_{n+1})\,,$$
$$\vdash (F \wedge K_n \wedge \neg J_{n+1}) \Rightarrow H_1 \qquad \text{et} \qquad \vdash H_1 \Rightarrow (G \wedge K_n \wedge \neg J_{n+1}).$$

Ce n'est pas possible car cela exige : $\vdash (F \wedge K_n) \Rightarrow (H_0 \vee H_1)$ et $\vdash (H_0 \vee H_1) \Rightarrow (G \wedge K_n)$, et $H_0 \vee H_1$ est alors une interpolante de $F \wedge K_n$ et $G \wedge K_n$.

On prendra alors K_{n+1} égale à $K_n \wedge J_{n+1}$ ou $K_n \wedge \neg J_{n+1}$ suivant le cas, de telle manière que $F \wedge K_{n+1}$ et $G \wedge K_{n+1}$ n'aient pas d'interpolante ; les conditions i), ii) et iii) sont bien vérifiées. Posons :

$$T = \{K_n \,;\, n \in \mathbb{N}\}.$$

On remarque que, pour tout n, $F \wedge K_n$ est une formule consistante : sinon, $\exists v_0 \neg v_0 \simeq v_0$ serait une interpolante entre $F \wedge K_n$ et $G \wedge K_n$. En utilisant la condition i) et le théorème de compacité, on voit que $\{F \cup T\}$ est une théorie consistante. De même, $\neg G \wedge K_n$ est consistante, sinon K_n serait une interpolante entre $F \wedge K_n$ et $G \wedge K_n$. Donc,

$T \cup \{\neg G\}$ est aussi consistante. Maintenant, il est clair que T est une théorie complète de L : si H est une formule close de L, il existe un entier n tel que $J_n = H$, et on s'est arrangé pour que $\vdash K_n \Rightarrow J_n$ ou $\vdash K_n \Rightarrow \neg J_n$.

☺

3.4 Le théorème d'interpolation de Craig conduit à l'important théorème de définissabilité de Beth. On commence par quelques remarques et notations.

On se donne un langage dénombrable L, un nouveau symbole de prédicat P d'arité n, et on pose $L' = L \cup \{P\}$. Soit P_1 un autre symbole de prédicat d'arité n ne figurant pas dans L. Si G est une formule de L', on notera $G_{P_1/P}$ la formule obtenue en substituant P_1 à toutes les occurrences de P dans G. On voit que, si F est une formule de L et si $\vdash F \Rightarrow G$, alors $\vdash F \Rightarrow G_{P_1/P}$.

Soit T une théorie dans le langage élargi L'. Il est à peu près clair que les deux conditions suivantes sont équivalentes :

- pour toute L-structure $\mathfrak{M}$, il y a au plus une interprétation de P qui enrichisse $\mathfrak{M}$ en un modèle de T.
- soient P_1 un nouveau symbole de prédicat d'arité n, $L_1 = L \cup \{P_1\}$ et T_1 la théorie obtenue en remplaçant P par P_1 dans T. Alors pour tout modèle $\mathfrak{N}$ de $T \cup T_1$, on a : $\mathfrak{N} \models \forall v_1 \forall v_2 \ldots \forall v_n (P v_1 v_2 \ldots v_n \Longleftrightarrow P_1 v_1 v_2 \ldots, v_n)$.

Cette dernière condition est encore équivalente à :

$$T \cup T_1 \vdash \forall v_1 \forall v_2 \ldots \forall v_n (P v_1 v_2 \ldots v_n \Longleftrightarrow P_1 v_1 v_2 \ldots v_n).$$

Si l'une de ces conditions est vérifiée, on dira que P est **implicitement définissable dans** T. On dira que P est **explicitement définissable dans** T s'il existe une formule $F[v_1, v_2, \ldots, v_n]$ de L telle que :

$$T \vdash \forall v_1 \forall v_2 \ldots \forall v_n (P v_1 v_2 \ldots v_n \Longleftrightarrow F[v_1, v_2, \ldots, v_n])$$

Il est bien évident que, si P est explicitement définissable dans T, alors il y est implicitement définissable. La réciproque de cette assertion est le **théorème de Beth** :

THEOREME : *Si* P *est implicitement définissable dans* T, *alors il y est explicitement définissable.*

☹ On garde les notations du paragraphe ci-dessus. On introduit n symboles de constante $c_1, c_2, \ldots, c_n$. Parce que P est implicitement définissable, la théorie :

$$T \cup \{P c_1 c_2 \ldots c_n\} \cup T_1 \cup \{\neg P_1 c_1 c_2 \ldots c_n\}$$

est contradictoire. A l'aide du théorème de compacité, on trouve des formules F de L' et G de L_1 telles que : $F \wedge G \wedge Pc_1c_2...c_n \wedge \neg P_1c_1c_2...c_n$ est contradictoire, $T \vdash F$ et $T_1 \vdash G$. Le fait que $F \wedge G \wedge Pc_1c_2...c_n \wedge \neg P_1c_1c_2...c_n$ est contradictoire peut se traduire par :

$$\vdash (F \wedge Pc_1c_2...c_n) \Longrightarrow (G \Longrightarrow P_1c_1c_2...c_n).$$

On applique le théorème d'interpolation : il existe une formule $H[v_1,v_2,...,v_n]$ de L (sans P ni P_1) telle que $H[c_1,c_2,...,c_n]$ soit une interpolante entre $F \wedge Pc_1c_2...c_n$ et $G \Longrightarrow P_1c_1c_2...c_n$. Comme $T \vdash F$, on a

$$T \vdash Pc_1c_2...c_n \Longrightarrow H[c_1,c_2,...,c_n],$$

et comme les constantes c_i n'apparaissent pas dans T :

$$T \vdash \forall v_1 \forall v_2 ... \forall v_n (Pv_1v_2...v_n \Longrightarrow H[v_1,v_2,...,v_n]).$$

De même :

$$T_1 \vdash \forall v_1 \forall v_2 ... \forall v_n (H[v_1,v_2,...,v_n] \Longrightarrow P_1v_1v_2...v_n),$$

et, en substituant P à P_1, on obtient :

$$T \vdash \forall v_1 \forall v_2 ... \forall v_n (H[v_1,v_2,...,v_n] \Longrightarrow Pv_1v_2...v_n).$$

☺

4. PRODUITS REDUITS ET ULTRAPRODUITS

4.1 Soient L un langage, I un ensemble et $(\mathfrak{M}_i)_{i \in I}$ une famille de L-structures. On va définir une autre L-structure, appelée **produit de la famille** $(\mathfrak{M}_i)_{i \in I}$ et notée $\prod_{i \in I} \mathfrak{M}_i$, dont l'ensemble de base est l'ensemble produit $\prod_{i \in I} M_i$. Fixons quelques notations d'abord : si a est un élément de $\prod_{i \in I} M_i$ et si $i \in I$, on notera a^i la i-ème coordonnée de a (autrement dit a est égal à la suite $(a^i ; i \in I)$) ; si X est un symbole (de constante, de fonction ou de prédicat) de L, alors X_i désigne l'interprétation de ce symbole dans $\mathfrak{M}_i$.

• Si c est un symbole de constante, alors l'interprétation de c dans $\prod_{i \in I} \mathfrak{M}_i$ est la suite $(c_i ; i \in I)$.

• Si f est un symbole de fonction d'arité n, alors l'interprétation de f dans $\prod_{i \in I} \mathfrak{M}_i$ est l'application qui à $(a_1,a_2,...,a_n)$ fait correspondre $(f_i(a_1^i,a_2^i,...,a_n^i) ; i \in I)$.

• Si R est un symbole de prédicat d'arité n, alors l'interprétation de R dans $\prod_{i \in I} \mathfrak{M}_i$ est l'ensemble

$$\{ (a_1,a_2,...,a_n) \in (\prod_{i \in I} M_i)^n \text{ ; pour tout } i \in I, (a_1^i,a_2^i,...,a_n^i) \in R_i \}.$$

On pourrait dire de façon plus condensée que la structure de $\prod_{i \in I} \mathfrak{M}_i$ est définie de telle sorte que, pour toute formule atomique $F[v_1,v_2,\ldots,v_n]$ et tous $a_1,a_2,\ldots,a_n$ de $\prod_{i \in I} M_i$,

$$\prod_{i \in I} \mathfrak{M}_i \models F[a_1,a_2,\ldots,a_n] \text{ si et seulement si pour tout } i \in I, \mathfrak{M}_i \models F[a_1^i,a_2^i,\ldots,a_n^i].$$

Lorsque l'ensemble I est fini, on parle de **produit fini**.

EXEMPLE : Si les $\mathfrak{M}_i$ sont des groupes, on retrouve le produit de groupes. Même chose avec les anneaux ou les ensembles ordonnés. On remarquera que le produit de corps n'est en général pas un corps (voir exercice 14) ; de même le produit d'ensembles totalement ordonnés n'est pas, en général, totalement ordonné.

4.2 On va maintenant généraliser cette définition. On se donne, en plus de l'ensemble I et des structures $\mathfrak{M}_i$, un filtre $\mathcal{F}$ de l'algèbre de Boole des parties de I. On considère sur $\prod_{i \in I} M_i$ la relation binaire $\approx_{\mathcal{F}}$ définie par :

$$(a^i ; i \in I) \approx_{\mathcal{F}} (b^i ; i \in I) \text{ si et seulement si } \{i \in I ; a^i = b^i\} \in \mathcal{F}.$$

On remarque que c'est une relation d'équivalence : elle est clairement symétrique et réflexive. Pour la transitivité, supposons que $(a^i ; i \in I)$, $(b^i ; i \in I)$ et $(c^i ; i \in I)$ soient trois éléments de $\prod_{i \in I} M_i$ et que :

$$(a^i ; i \in I) \approx_{\mathcal{F}} (b^i ; i \in I) \text{ et } (b^i ; i \in I) \approx_{\mathcal{F}} (c^i ; i \in I) ;$$

cela veut dire que :

$$\{i \in I ; a^i = b^i\} \in \mathcal{F} \text{ et } \{i \in I ; b^i = c^i\} \in \mathcal{F}.$$

Or $\{i \in I ; a^i = b^i\} \cap \{i \in I ; b^i = c^i\} \subseteq \{i \in I ; a^i = c^i\}$, et, puisque $\mathcal{F}$ est un filtre, on voit bien que $\{i \in I ; a^i = c^i\} \in \mathcal{F}$.

On notera $\prod_{i \in I} M_i/\mathcal{F}$ l'ensemble des classes d'équivalence de $\prod_{i \in I} M_i$ relativement à cette relation. Si $a \in \prod_{i \in I} M_i$, on notera $\bar{a}$ la classe de a modulo $\approx_{\mathcal{F}}$, à condition que cela ne crée aucune ambiguïté.

On va maintenant définir sur l'ensemble $\prod_{i \in I} M_i/\mathcal{F}$ une L-structure, que l'on notera $\prod_{i \in I} \mathfrak{M}_i/\mathcal{F}$ et que l'on appellera **le produit réduit de la famille $(\mathfrak{M}_i)_{i \in I}$ modulo le filtre $\mathcal{F}$** ; cette définition sera telle que, pour toute formule atomique $F[v_1,v_2,\ldots,v_n]$ et pour tous $a_1,a_2,\ldots,a_n$ de $\prod_{i \in I} M_i$:

$$\prod_{i \in I} \mathfrak{M}_i/\mathcal{F} \models F[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n] \text{ si et seulement si } \{i \in I ; \mathfrak{M}_i \models F[a_1^i,a_2^i,\ldots,a_n^i]\} \in \mathcal{F}.$$

• Tout d'abord, si c est un symbole de constante, alors l'interprétation de c dans $\prod_{i \in I} \mathfrak{M}_i/\mathcal{F}$ est la classe modulo $\approx_{\mathcal{F}}$ de la suite $(c_i ; i \in I)$.

• Soient R un symbole de prédicat d'arité n et $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n$ des points de $\prod_{i \in I} \mathfrak{M}_i / \mathcal{F}$. Soit, pour chaque k compris entre 1 et n, $(b^i_k\,;\, i \in I)$ un autre représentant dans $\prod_{i \in I} M_i$ de $\bar{a}_k$. Alors :

$$\{i \in I\,;\, \text{pour tout } k \text{ compris entre 1 et } n,\ a^i_k = b^i_k\} \in \mathcal{F},$$

et par conséquent,

$$\{i \in I\,;\, \mathfrak{M}_i \models R a^i_1 a^i_2 \ldots a^i_n\} \in \mathcal{F} \text{ si et seulement si } \{i \in I\,;\, \mathfrak{M}_i \models R b^i_1 b^i_2 \ldots b^i_n\} \in \mathcal{F}.$$

Il est donc légitime et naturel de décider que :

$$\prod_{i \in I} \mathfrak{M}_i / \mathcal{F} \models R \bar{a}_1 \bar{a}_2 \ldots \bar{a}_n \ \text{ si et seulement si } \{i \in I\,;\, \mathfrak{M}_i \models R a^i_1 a^i_2 \ldots a^i_n\} \in \mathcal{F}.$$

• Soient maintenant f un symbole de fonction d'arité n et $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n$ des points de $\prod_{i \in I} M_i / \mathcal{F}$. On remarque encore que si, pour tout k compris entre 1 et n, $(b^i_k\,;\, i \in I)$ est un autre représentant de a_k, alors :

$$(f_i(a^i_1, a^i_2, \ldots, a^i_n)\,;\, i \in I) \approx_{\mathcal{F}} (f_i(b^i_1, b^i_2, \ldots, b^i_n)\,;\, i \in I).$$

L'interprétation de f dans $\prod_{i \in I} \mathfrak{M}_i / \mathcal{F}$ est l'application qui à $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n$ fait correspondre la classe de $(f_i(a^i_1, a^i_2, \ldots, a^i_n)\,;\, i \in I)$ relativement à $\approx_{\mathcal{F}}$.

EXEMPLE : Le produit défini en 4.1 est un cas particulier de produit réduit : il correspond au cas où $\mathcal{F}$ a pour unique élément l'ensemble I tout entier. On verra que les produits réduits de groupes, d'anneaux ou d'ensembles ordonnnés sont respectivement des groupes, des anneaux ou des ensembles ordonnés. On verra aussi (exercice 14) qu'un produit réduit de corps n'est que très rarement un corps.

Dans le cas où toutes les structures $\mathfrak{M}_i$ sont égales à une même structure $\mathfrak{M}$, on parlera de **puissance réduite de $\mathfrak{M}$ modulo $\mathcal{F}$**. On la désignera par $\mathfrak{M}^I / \mathcal{F}$.

4.3 Si $\mathcal{F}$ est un ultrafiltre, alors $\prod_{i \in I} \mathfrak{M}_i / \mathcal{F}$ est appelé l'**ultraproduit de la famille $(\mathfrak{M}_i)_{i \in I}$ modulo $\mathcal{F}$**, et si toutes les structures $\mathfrak{M}_i$ sont égales à une même structure $\mathfrak{M}$, on parlera d'**ultrapuissance de $\mathfrak{M}$ modulo $\mathcal{F}$** (et on écrira conformément à la convention précédente $\mathfrak{M}^I / \mathcal{F}$). L'intéret des ultraproduits réside dans le théorème suivant, appelé **théorème de Łos** :

THEOREME : *Soient $(\mathfrak{M}_i\,;\, i \in I)$ une famille de L-structures et $\mathcal{F}$ un ultrafiltre sur I. Alors, pour toute formule $F[v_1, v_2, \ldots, v_n]$ de L et tous éléments $a_1, a_2, \ldots, a_n$ de $\prod_{i \in I} M_i$,*

$$\prod_{i \in I} \mathfrak{M}_i / \mathcal{F} \models F[\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n] \text{ si et seulement si } \{i \in I\,;\, \mathfrak{M}_i \models F[a^i_1, a^i_2, \ldots, a^i_n]\} \in \mathcal{F}.$$

☹ On peut supposer d'abord que les seuls connecteurs propositionnels apparaissant dans F sont $\neg$ et $\wedge$ et que le quantificateur universel n'y apparaît pas. La preuve se fait alors par induction sur la hauteur de F. On a déjà le résultat si F est une formule atomique.

• Cas où $F[v_1,v_2,\ldots,v_n] = \neg G[v_1,v_2,\ldots,v_n]$. Pour tous éléments $a_1,a_2,\ldots,a_n$ de $\prod_{i\in I} M_i$,

$$\prod_{i\in I} \mathfrak{M}_i/\mathcal{F} \models F[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n] \text{ si et seulement si } \prod_{i\in I} \mathfrak{M}_i/\mathcal{F} \not\models G[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n],$$

et donc, par hypothèse d'induction, si et seulement si $\{i \in I \,;\, \mathfrak{M}_i \models G[a_1^i,a_2^i,\ldots,a_n^i]\} \notin \mathcal{F}$. Or $\mathcal{F}$ est un ultrafiltre, donc $\{i \in I \,;\, \mathfrak{M}_i \models G[a_1^i,a_2^i,\ldots,a_n^i]\} \notin \mathcal{F}$ si et seulement si son complémentaire appartient à $\mathcal{F}$. Donc :

$$\prod_{i\in I} \mathfrak{M}_i/\mathcal{F} \models F[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n] \text{ si et seulement si } \{i \in I \,;\, \mathfrak{M}_i \models F[a_1^i,a_2^i,\ldots,a_n^i]\} \in \mathcal{F}.$$

• Cas où $F[v_1,v_2,\ldots,v_n] = G[v_1,v_2,\ldots,v_n] \wedge H[v_1,v_2,\ldots,v_n]$. Alors, pour tous éléments $a_1,a_2,\ldots,a_n$ de $\prod_{i\in I} M_i$,

$$\prod_{i\in I} \mathfrak{M}_i/\mathcal{F} \models F[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n]$$

si et seulement si

$$\prod_{i\in I} \mathfrak{M}_i/\mathcal{F} \models G[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n] \text{ et } \prod_{i\in I} \mathfrak{M}_i/\mathcal{F} \models H[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n].$$

Par hypothèse d'induction, ceci est encore équivalent à :

$$\{i \in I \,;\, \mathfrak{M}_i \models G[a_1^i,a_2^i,\ldots,a_n^i]\} \in \mathcal{F} \text{ et } \{i \in I \,;\, \mathfrak{M}_i \models H[a_1^i,a_2^i,\ldots,a_n^i]\} \in \mathcal{F}.$$

Or $\mathcal{F}$ est un filtre ; donc ces ensembles appartiennent tous les deux à $\mathcal{F}$ si et seulement si leur intersection appartient à $\mathcal{F}$, et leur intersection est égale à :

$$\{i \in I \,;\, \mathfrak{M}_i \models F[a_1^i,a_2^i,\ldots,a_n^i]\}.$$

• Cas où $F = \exists v_0 G[v_0,v_1,\ldots,v_n]$. Soient $a_1,a_2,\ldots,a_n$ des éléments de $\prod_{i\in I} M_i$ et supposons que :

$$\prod_{i\in I} \mathfrak{M}_i/\mathcal{F} \models F[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n].$$

Alors, il existe $a_0 \in \prod_{i\in I} M_i$ tel que $\prod_{i\in I} \mathfrak{M}_i/\mathcal{F} \models G[\bar{a}_0,\bar{a}_1,\ldots,\bar{a}_n]$. Par hypothèse d'induction, on voit donc que l'ensemble $X = \{i \in I \,;\, \mathfrak{M}_i \models G[a_0^i,a_1^i,\ldots,a_n^i]\}$ appartient à $\mathcal{F}$. Il est clair que si $i \in X$, $\mathfrak{M}_i \models \exists v_0 G[v_0,\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n]$, et donc l'ensemble $\{i \in I \,;\, \mathfrak{M}_i \models F[a_1^i,a_2^i,\ldots,a_n^i]\}$ contient X et appartient à $\mathcal{F}$.

Réciproquement, supposons que $Y = \{i \in I \,;\, \mathfrak{M}_i \models F[a_1^i,a_2^i,\ldots,a_n^i]\} \in \mathcal{F}$. On définit une suite $a_0 = (a_0^i \,;\, i \in I)$ de la façon suivante : si $i \in Y$, a_0^i est un point de M_i tel que $\mathfrak{M}_i \models G[a_0^i,a_1^i,\ldots,a_n^i]$; si $i \notin Y$, on donne à a_0^i n'importe quelle valeur. On voit alors que $\{i \in I \,;\, \mathfrak{M}_i \models G[a_0^i,a_1^i,\ldots,a_n^i]\}$ contient Y, donc appartient à $\mathcal{F}$ et, par hypothèse d'induction, $\prod_{i\in I} \mathfrak{M}_i/\mathcal{F} \models G[\bar{a}_0,\bar{a}_1,\ldots,\bar{a}_n]$.

☺

4.4 La construction des produits réduits et des ultraproduits est purement algébrique, et on a besoin de très peu de choses pour établir le théorème de Łos. L'argument qui suit donne une nouvelle preuve du théorème de compacité. Cette preuve est débarrassée de toute considération syntaxique, contrairement à celle qui a déjà été donnée qui s'appuie sur le théorème de complétude.

COROLLAIRE : *Soit* T *une théorie dont tout sous-ensemble fini a un modèle. Alors* T *a un modèle.*

☹ Appelons I l'ensemble des parties finies de T. Pour chaque $i \in I$, choisissons un modèle de $\mathfrak{M}_i$, de i (on sait qu'il en existe).

Maintenant, pour chaque formule F de T, considérons le sous-ensemble X(F) suivant de I :

$$X(F) = \{i \in I\ ;\ F \in i\}.$$

On voit que l'intersection d'un nombre fini d'ensembles de la forme X(F) n'est jamais vide : en effet, si $F_1, F_2, \ldots, F_n$ sont dans T, alors $\{F_1, F_2, \ldots, F_n\}$ appartient à $\bigcap_{1 \leqslant i \leqslant n} X(F_i)$. L'ensemble $\{ X(F)\ ;\ F \in T \}$ est donc une base de filtre, et on peut trouver un ultrafiltre $\mathcal{F}$ contenant cet ensemble (chapitre 2, théorème 5.13). On utilise le théorème de Łos pour vérifier que $\prod_{i \in I} \mathfrak{M}_i / \mathcal{F}$ est un modèle de T : en effet, si $F \in T$, $\{i \in I\ ;\ \mathfrak{M}_i \models F\}$ contient X(F) et appartient donc à $\mathcal{F}$.

☺

4.5 La proposition suivante dit qu'une ultrapuissance de $\mathfrak{M}$ peut être considérée comme une extension élémentaire de $\mathfrak{M}$:

PROPOSITION : *Soient* $\mathfrak{M}$ *une* L*-structure,* I *un ensemble et* $\mathcal{F}$ *un ultrafiltre sur* I. *Pour* $a \in M$, *appelons* c(a) *l'application de* I *dans* M *constante et égale à* a, *et* h(a) *la classe de* c(a) *modulo* $\approx_{\mathcal{F}}$. *Alors* h *est une application élémentaire de* $\mathfrak{M}$ *dans* $\mathfrak{M}^I / \mathcal{F}$.

☹ Moyennant le théorème de Łos, cela revient à dire que pour toute formule $F[v_1, v_2, \ldots, v_n]$ de L et tous éléments $a_1, a_2, \ldots, a_n$ de M :

$\mathfrak{M} \models F[a_1, a_2, \ldots, a_n]$ si et seulement si $\{ i \in I\ ;\ \mathfrak{M} \models F[c(a_1)^i, c(a_2)^i, \ldots, c(a_n)^i] \} \in \mathcal{F}$.

C'est donc évident puisque, pour tout $i \in I$ et pour tout k compris entre 1 et n, $c(a_k)^i$ est égal à a_k.

☺

5. THEOREMES DE PRESERVATION

Préservation par sous-structure

5.1 Les théorèmes de préservation sont des résultats qui relient la forme syntaxique d'une théorie aux propriétés de clôture de la classe de ses modèles. Le plus facile, par lequel on va commencer, concerne la préservation des formules universelles. Le problème a déjà été abordé au chapitre 3 (5.1, théorème 2). Rappelons une définition :

> DEFINITION : *Une* ***formule universelle*** *est une formule prénexe dans laquelle le quantificateur existentiel n'a pas d'occurrence. Une* ***théorie universelle*** *est une théorie composée uniquement de formules universelles.*

Par exemple, la théorie des ordres totaux (axiomes (i), (ii), (iii) de 1.3) est une théorie universelle. Les groupes offrent un exemple intéressant. Dans le langage composé d'un symbole de constante 1 et d'un symbole de fonction binaire $\cdot$, les axiomes en sont :

(i) $\forall v_1 \forall v_2 \forall v_3 \, (v_1 \cdot v_2) \cdot v_3 \simeq v_1 \cdot (v_2 \cdot v_3)$;

(ii) $\forall v_1 (v_1 \cdot 1 \simeq v_1 \wedge 1 \cdot v_1 \simeq v_1)$;

(iii) $\forall v_1 \exists v_2 (v_1 \cdot v_2 \simeq 1 \wedge v_2 \cdot v_1 \simeq 1)$.

Il ne s'agit donc pas d'une théorie universelle, à cause du troisième axiome. Toutefois, on peut choisir d'inclure dans le langage un symbole de fonction unaire $^{-1}$ pour désigner la fonction inverse. Dans ce cas, le troisième axiome doit être remplacé par :

(iii bis) $\forall v_1 (v_1 \cdot v_1^{-1} \simeq 1 \wedge v_1^{-1} \cdot v_1 \simeq 1)$,

ce qui, cette fois, donne une axiomatisation universelle.

REMARQUE : La conjonction de deux formules universelles n'est pas en général une formule universelle. Cependant, elle est équivalente à une formule universelle. En effet :

$\forall v_1 \forall v_2 \ldots \forall v_n F_1 \wedge \forall w_1 \forall w_2 \ldots \forall w_p F_2$ est équivalente à $\forall v_1 \forall v_2 \ldots \forall v_n \forall w_1 \forall w_2 \ldots \forall w_p (F_1 \wedge F_2)$

pourvu que les v_i (pour i compris entre 1 et n) n'aient pas d'occurrence libre dans F_2 et que les w_j (pour j compris entre 1 et p) n'aient pas d'occurrences libres dans F_1. Quitte à renommer les variables liées, on peut toujours supposer que cette condition est satisfaite. La conjonction d'un nombre fini de formules universelles est aussi équivalente à une formule universelle. De même pour la disjonction de formules universelles :

$\forall v_1 \forall v_2 \ldots \forall v_n F_1 \vee \forall w_1 \forall w_2 \ldots \forall w_p F_2$ est équivalente à $\forall v_1 \forall v_2 \ldots \forall v_n \forall w_1 \forall w_2 \ldots \forall w_p (F_1 \vee F_2)$

si la condition mentionnée plus haut est encore vérifiée.

5.2 DEFINITION : *On dit qu'une théorie* T **est préservée par sous-structure** *si, pour tout modèle* $\mathfrak{M}$ *de* T *et toute sous-structure* $\mathfrak{N}$ *de* $\mathfrak{M}$, $\mathfrak{N}$ *est un modèle de* T. *Une formule close* F **est préservée par sous-structure** *si la théorie* $\{F\}$ *l'est.*

Voici donc **le théorème de préservation des formules universelles** promis :

THEOREME : *Soit* T *une théorie dans un langage* L ; *alors les deux conditions suivantes sont équivalentes :*

i) *Il existe une théorie universelle* Ψ *dans* L *équivalente à* T.

ii) *La théorie* T *est préservée par sous-structure.*

☹ Le sens *i)* ⟹ *ii)* a été établi au chapitre 3 (5.1, théorème 2). Pour la réciproque, on reprend une idée déjà exposée dans l'exercice 19 du chapitre 3. Supposons que *ii)* soit vérifiée. Posons :

$$\Psi = \{ G \ ; G \text{ est une formule universelle close et } T \vdash G \}.$$

Il est clair que toute formule de Ψ est conséquence de T . On va montrer que tout modèle de Ψ est un modèle de T. Soit donc $\mathfrak{M}$ un modèle de Ψ. Considérons le diagramme simple de $\mathfrak{M}$:

$$\Delta(\mathfrak{M}) = \{ H[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n] \ ; H \text{ est une formule sans quantificateur et } \mathfrak{M} \models H[a_1,a_2,\ldots,a_n] \}.$$

Il suffit de montrer que $\Delta(\mathfrak{M}) \cup T$ a un modèle : on a vu que, dans ce cas, $\Delta(\mathfrak{M}) \cup T$ a un modèle qui est une extension de $\mathfrak{M}$ (lemme 2.3). Avec l'hypothèse *ii)*, cela montre que $\mathfrak{M}$ est un modèle de T.

Supposons que $\Delta(\mathfrak{M}) \cup T$ n'est pas consistante ; il existe des formules sans quantificateur $H_1[v_1,v_2,\ldots,v_n]$, $H_2[v_1,v_2,\ldots,v_n]$, ..., $H_p[v_1,v_2,\ldots,v_n]$ et des points $a_1,a_2,\ldots,a_n$ dans M tels que :

$$T \vdash \neg(H_1[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n] \wedge H_2[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n] \wedge \ldots \wedge H_p[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n])$$

et $$\mathfrak{M} \models H_1[a_1,a_2,\ldots,a_n] \wedge H_2[a_1,a_2,\ldots,a_n] \wedge \ldots \wedge H_p[a_1,a_2,\ldots,a_n]$$

Mais, puisque les symboles $\underline{a}_i$, pour $1 \leqslant i \leqslant n$, n'apparaissent pas dans T, on a :

$$T \vdash \forall v_1 \forall v_2 \ldots \forall v_n \neg(H_1[v_1,v_2,\ldots,v_n] \wedge H_2[v_1,v_2,\ldots,v_n] \wedge \ldots \wedge H_p[v_1,v_2,\ldots,v_n])$$

ce qui prouve que $\forall v_1 \forall v_2 \ldots \forall v_n \neg(H_1[v_1,v_2,\ldots,v_n] \wedge H_2[v_1,v_2,\ldots,v_n] \wedge \ldots \wedge H_p[v_1,v_2,\ldots,v_n])$ est une formule de Ψ. Ceci contredit le fait que $\mathfrak{M}$ est un modèle de Ψ.

☺

Reprenons l'exemple des groupes. Si le langage est $\{1, \cdot\}$, alors il est faux que toute sous-structure d'un groupe est un groupe : par exemple, $\mathbb{N}$ est une sous-structure de $\mathbb{Z}$ et n'en est pas un sous-groupe ; cela montre que, dans ce langage, la théorie des

groupes n'est pas équivalente à une théorie universelle. Mais si on ajoute au langage la fonction inverse, la notion de sous-structure change (une sous-structure doit être close pour toutes les fonctions du langage), et alors une sous-structure d'un groupe est nécessairement un groupe, ce qui n'est pas étonnant puisqu'on a, dans ce cas, une axiomatisation universelle.

5.3 COROLLAIRE : *Soit* F *une formule close dans un langage* L ; *alors les deux conditions suivantes sont équivalentes* :

i) Il existe une formule universelle close G *dans* L *équivalente à* F.

ii) La formule F *est préservée par sous-structure.*

☹ Le sens *i)* $\Longrightarrow$ *ii)* est contenu dans le théorème précédent. Supposons donc *ii)*. Le théorème précédent nous dit encore qu'il existe une théorie universelle Ψ équivalente à F. Par compacité, il existe une partie finie Ψ_0 de Ψ équivalente à F qui est donc équivalente à la conjonction des formules de Ψ_0, elle-même équivalente, par la remarque 5.1, à une formule universelle.

☺

5.4 Ces théorèmes admettent un dual : on dit qu'une formule close F (ou qu'une théorie T) est **preservée par extension** si, pour tout modèle $\mathfrak{M}$ de F (de T) et toute extension $\mathfrak{N}$ de $\mathfrak{M}$, $\mathfrak{N}$ est un modèle de F (de T). D'autre part, une formule **existentielle** est une formule prénexe dans laquelle le quantificateur universel n'a pas d'occurrence et une **théorie existentielle** est une théorie constituée de formules existentielles. Alors, on voit qu'une formule est équivalente à une formule existentielle si et seulement si sa négation est équivalente à une formule universelle, et qu'une formule est préservée par extension si et seulement si sa négation est préservée par sous-structure. De tout cela on déduit **le théorème de préservation des formules existentielles** :

THEOREME : *Une formule close est préservée par extension si et seulement si elle est équivalente à une formule existentielle.*

On a un théorème analogue pour les théories : *une théorie est préservée par extension si et seulement si elle est équivalente à une théorie existentielle.* La partie « si » est facile, mais pour établir l'autre implication, la dualité avec les formules universelles ne suffit pas. Il faut travailler un peu plus : c'est l'objet de l'exercice 17.

Présevation par union de chaîne

5.5 Passons maintenant à quelque chose de plus compliqué :

DEFINITION : *Une* ***formule*** $\forall\exists$ *(lire pour tout il existe) est une formule prénexe de la forme*

$$\forall v_1 \forall v_2 \ldots \forall v_n \exists v_{n+1} \exists v_{n+2} \ldots \exists v_{n+p} G ,$$

où G *est une formule sans quantificateur. Un* ***théorie*** $\forall\exists$ *est une théorie constituée de formules* $\forall\exists$.

Une formule $\forall\exists$ commence donc par un certain nombre (éventuellement zéro) de quantificateurs universels qui sont suivis de quantificateurs existentiels qui eux-même sont suivis d'une formule sans quantificateur. Les formules universelles ou existentielles sont des cas particuliers de formules $\forall\exists$.

Remarquons encore que la conjonction ou la disjonction d'un nombre fini de formules $\forall\exists$ est équivalente à une formule $\forall\exists$ (ce qui se démontre sans peine, toujours en renommant les variables liées).

5.6 DEFINITION : *On dit qu'une* ***théorie*** T ***est préservée par union de chaîne*** *si toute union de chaîne de modèles de* T *est encore un modèle de* T. *Une* ***formule close*** F ***est préservée par union de chaîne*** *si la théorie* { F } *l'est.*

En paraphrasant, T est préservée par union de chaîne si et seulement si la condition suivante est vérifiée :

• Si $(I,<)$ est un ensemble totalement ordonné et si $(\mathfrak{M}_i \,;\, i \in I)$ est une famille de modèles de T telle que, pour tout éléments i et j de I, $i < j$ implique $\mathfrak{M}_i \subseteq \mathfrak{M}_j$, alors $\bigcup_{i \in I} \mathfrak{M}_i$ est un modèle de T.

THEOREME : *Une théorie est préservée par union de chaîne si et seulement si elle est équivalente à une théorie* $\forall\exists$.

☺ On va d'abord voir qu'une formule close $\forall\exists$ est préservée par union de chaîne ; cela impliquera clairement que les formules closes équivalentes à une formule close $\forall\exists$ et que les théories équivalentes à une théorie $\forall\exists$ sont aussi préservées par union de chaîne.

Considérons donc la formule $F = \forall v_1 \forall v_2 \ldots \forall v_n \exists v_{n+1} \exists v_{n+2} \ldots \exists v_{n+p} H[v_1, v_2, \ldots, v_{n+p}]$, où H est une formule sans quantificateur. Soient $(I,<)$ un ensemble totalement ordonné et $(\mathfrak{M}_i\ ;\ i \in I)$ une chaîne de modèles de F. Posons $\mathfrak{M} = \bigcup_{i \in I} \mathfrak{M}_i$. Il s'agit de montrer que $\mathfrak{M}$ est un modèle de F. Pour cela, prenons des éléments quelconques $a_1, a_2, \ldots, a_n$ de M et montrons que :

$$\mathfrak{M} \models \exists v_{n+1} \exists v_{n+2} \ldots \exists v_{n+p} H[a_1, a_2, \ldots a_n, v_{n+1}, v_{n+2}, \ldots, v_{n+p}].$$

Puisque la famille $(\mathfrak{M}_i\ ;\ i \in I)$ est totalement ordonnée par inclusion, il existe un indice $i \in I$ tel que tous les a_k, pour k compris entre 1 et n, sont contenus dans M_i. Parce que $\mathfrak{M}_i$ est un modèle de F, il existe des points a_{n+1}, $a_{n+2}, \ldots, a_{n+p}$ dans M_i tels que : $\mathfrak{M}_i \models H[a_1, a_2, \ldots, a_{n+p}]$; alors $\mathfrak{M} \models H[a_1, a_2, \ldots, a_{n+p}]$ parce que H est sans quantificateur et que $\mathfrak{M}$ est une extension de $\mathfrak{M}_i$. On voit donc que $\mathfrak{M} \models F$.

Pour la réciproque, on va montrer qu'une théorie T préservée par union de chaîne est équivalente à une théorie $\forall\exists$. Posons :

$$\Psi = \{ G\ ;\ G \text{ est une formule } \forall\exists \text{ close et } T \vdash G \}.$$

Il est clair que toute formule de Ψ est conséquence de T, et on va voir que l'inverse est vrai. On commence par une définition et deux lemmes.

5.7 DEFINITION : *Soient* $\mathfrak{M}$ *et* $\mathfrak{N}$ *deux* L-*structures telles que* $\mathfrak{M} \subseteq \mathfrak{N}$. *On dit que* $\mathfrak{M}$ *est une* **sous-structure 1-élémentaire** *de* $\mathfrak{N}$ *et on écrit* $\mathfrak{M} \prec_1 \mathfrak{N}$ *si, pour toute formule universelle* $F[v_1, v_2, \ldots, v_n]$ *de* L *et tous éléments* a_1, a_2, ..., a_n *de* M, *si* $\mathfrak{M} \models F[a_1, a_2, \ldots, a_n]$ *alors* $\mathfrak{N} \models F[a_1, a_2, \ldots, a_n]$.

On voit facilement que si $\mathfrak{M}$ est une sous-structure 1-élémentaire de $\mathfrak{N}$, alors pour toute formule universelle (ou existentielle) $F[v_1, v_2, \ldots, v_n]$ de L et tous éléments a_1, a_2, ..., a_n de M,

$$\mathfrak{M} \models F[a_1, a_2, \ldots, a_n] \text{ si et seulement si } \mathfrak{N} \models F[a_1, a_2, \ldots, a_n].$$

Cela justifie le terme de 1-élémentaire (élémentaire pour les formules à un seul bloc de quantificateurs).

LEMME 1 : *Supposons que* $\mathfrak{M} \prec_1 \mathfrak{N}$. *Alors il existe* $\mathfrak{M}'$ *telle que* $\mathfrak{M} \prec \mathfrak{M}'$ *et* $\mathfrak{N} \subseteq \mathfrak{M}'$.

☺ On utilise la méthode des diagrammes. On considère les théories suivantes dans L_N (le diagramme simple de $\mathfrak{N}$ et le diagramme complet de $\mathfrak{M}$) :

$\Delta(\mathfrak{N}) = \{ H[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n]$; H est une formule de L sans quantificateur, a_1, a_2, ..., a_n sont des points de N et $\mathfrak{N} \models H[a_1,a_2,\ldots,a_n] \}$,

et $D(\mathfrak{M}) = \{ F[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n]$; F est une formule de L , a_1, a_2, ..., a_n sont des points de M et $\mathfrak{M} \models H[a_1,a_2,\ldots,a_n] \}$.

On va montrer que $\Delta(\mathfrak{N}) \cup D(\mathfrak{M})$ est une théorie consistante ; on aura alors terminé, car, grâce au lemme 2.3, on aura une extension (simple) de $\mathfrak{N}$ qui est un modèle de $D(\mathfrak{M})$, c'est-à-dire une extension élémentaire de $\mathfrak{M}$.

L'ensemble $\Delta(\mathfrak{N})$ est clos par conjonction. En utilisant le théorème de compacité, on voit que, si l'on suppose que $\Delta(\mathfrak{N}) \cup D(\mathfrak{M})$ n'est pas consistant, alors on obtient une formule de $\Delta(\mathfrak{N})$, écrite sous la forme $H[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n,\underline{a}_{n+1},\ldots,\underline{a}_{n+p}]$, où H est sans quantificateur, $a_1,a_2,\ldots,a_n$ sont des points de M et $a_{n+1},a_{n+2},\ldots,a_{n+p}$ sont des points de N - M, telle que :

$$D(\mathfrak{M}) \vdash \neg H[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n,\underline{a}_{n+1},\ldots,\underline{a}_{n+p}].$$

Puisque les a_i, pour i compris entre $n + 1$ et $n + p$, n'apparaissent pas dans $D(\mathfrak{M})$, on a :

$$D(\mathfrak{M}) \vdash \forall v_1 \forall v_2 \ldots \forall v_p \neg H[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n,v_1,\ldots,v_p]$$

et donc :

$$\mathfrak{M} \models \forall v_1 \forall v_2 \ldots \forall v_p \neg H[a_1,a_2,\ldots,a_n,v_1,\ldots,v_p].$$

Or cette formule n'est manifestement pas satisfaite dans $\mathfrak{N}$ (puisque la formule $H[a_1,a_2,\ldots,a_n,a_{n+1},\ldots,a_{n+p}]$ y est satisfaite), et cela contredit le fait que $\mathfrak{M} \prec_1 \mathfrak{N}$.

☺

LEMME 2 : *Soit $\mathfrak{N}$ un modèle de Ψ. Alors il existe une extension 1-élémentaire de $\mathfrak{N}$ qui est modèle de* T.

☺ Considérons la théorie :

$\Delta_1(\mathfrak{N}) = \{ H[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n]$; H est la conjonction de formules universelles de L, a_1 ,a_2 ,..., a_n sont des points de N et $\mathfrak{N} \models H[a_1,a_2,\ldots,a_n] \}$.

On voit d'abord que $\Delta_1(\mathfrak{N}) \cup T$ est une théorie consistante : sinon, il existe une formule $H[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n]$ de $\Delta_1(\mathfrak{N})$ (qui est clos par conjonction) telle que :

$$T \vdash \neg H[\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_n],$$

et puisque les a_i, pour i compris entre 1 et n, n'apparaissent pas dans T :

$$T \vdash \forall v_1 \forall v_2 \ldots \forall v_n \neg H[v_1,v_2,\ldots,v_n].$$

Comme H est équivalente à une formule universelle, $\neg H[v_1,v_2,\ldots,v_n]$ est équivalente à une formule existentielle et $\forall v_1 \forall v_2 \ldots \forall v_n \neg H[v_1,v_2,\ldots,v_n]$ est équivalente à une formule $\forall\exists$ qui appartient à Ψ, par définition de ce dernier ensemble. On obtient une contradiction avec le fait que $\mathfrak{N}$ est modèle de Ψ.

On peut donc trouver un modèle $\mathfrak{M}$ de $\Delta_1(\mathfrak{N}) \cup T$ que l'on peut supposer, toujours grâce à ce même lemme 2.3, être une extension de $\mathfrak{N}$. Le fait que ce soit un modèle de $\Delta_1(\mathfrak{N})$ montre immédiatement que $\mathfrak{N} \prec_1 \mathfrak{M}$.

☺

On peut maintenant montrer que tout modèle de Ψ est modèle de T : on part d'un modèle $\mathfrak{M}_0$ de Ψ. Grâce au lemme 2, on trouve un modèle $\mathfrak{M}_1$ de T tel que $\mathfrak{M}_0 \prec_1 \mathfrak{M}_1$. On utilise ensuite le lemme 1 pour trouver une extension élémentaire $\mathfrak{M}_2$ de $\mathfrak{M}_0$ (qui est donc un modèle de Ψ) qui est aussi une extension de $\mathfrak{M}_1$. On continue en appliquant alternativement les lemmes 2 et 1 et on construit ainsi une chaîne $(\mathfrak{M}_k ; k \in \mathbb{N})$ de L-structures telle que, pour tout k, $\mathfrak{M}_{2k}$ est un modèle de Ψ, $\mathfrak{M}_{2k+1}$ est un modèle de T, $\mathfrak{M}_{2k} \prec_1 \mathfrak{M}_{2k+1}$ et $\mathfrak{M}_{2k} \prec \mathfrak{M}_{2k+2}$.

Posons $\mathfrak{M} = \bigcup_{k \in \mathbb{N}} \mathfrak{M}_k$. On remarque que $\mathfrak{M}$ est aussi égale à $\bigcup_{k \in \mathbb{N}} \mathfrak{M}_{2k}$ et à $\bigcup_{k \in \mathbb{N}} \mathfrak{M}_{2k+1}$. Puisque T est préservée par union de chaîne, $\mathfrak{M}$ est un modèle de T. D'après le théorème de l'union de chaîne de Tarski (2.9), puisque la chaîne $(\mathfrak{M}_{2k} ; k \in \mathbb{N})$ est élémentaire, $\mathfrak{M}$ est une extension élémentaire de $\mathfrak{M}_0$, donc $\mathfrak{M}_0$ est aussi un modèle de T.

☺

REMARQUE : Dans le raisonnement précédent, on a seulement utilisé le fait que T était préservée par union de chaîne indexée par les entiers. Autrement dit, on a aussi montré :

Si pour toute suite croissante $(\mathfrak{M}_n ; n \in \mathbb{N})$ de modèles de T, $\bigcup_{n \in \mathbb{N}} \mathfrak{M}_n$ est un modèle de T, alors T est équivalente à une théorie $\forall\exists$.

5.8 Comme exemple de théorie $\forall\exists$ (donc préservée par union de chaîne), il y a les théories des groupes, des corps, des ordres, des ordres denses sans extrémités. En revanche, la théorie des ordres denses avec un premier et un dernier élément n'est pas préservée par union de chaîne. Voici une axiomatisation de cette théorie :

(i) $\forall v_0(\neg v_0 < v_0)$

(ii) $\forall v_0 \forall v_1((v_0 < v_1 \Longleftrightarrow \neg v_1 < v_0) \vee v_0 = v_1)$

(iii) $\forall v_0 \forall v_1 \forall v_2((v_0 < v_1 \wedge v_1 < v_2) \Longrightarrow v_0 < v_2)$

(iv) $\neg\forall v_0 \exists v_1\, v_0 < v_1$

(v) $\neg\forall v_0 \exists v_1\, v_1 < v_0$

(vi) $\forall v_0 \forall v_1 \exists v_2(v_0 < v_1 \Longrightarrow (v_0 < v_2 \wedge v_2 < v_1))$.

Pour chaque entier i strictement positif, soit $\mathfrak{M}_i$ l'intervalle réel $[-i,+i]$; on voit que chaque $\mathfrak{M}_i$ est un modèle de la théorie ci-dessus, mais que l'union des $\mathfrak{M}_i$ est $\mathbb{R}$ tout entier et n'a ni plus grand ni plus petit élément. Cela montre que l'on ne peut pas trouver d'axiomatisation $\forall\exists$ de la notion d'ordre dense avec premier et dernier élément.

5.9 Un raisonnement par compacité, analogue à celui du corollaire 5.3 donne :

THEOREME : *Une formule close est préservée par union de chaîne si et seulement si elle est équivalente à une formule close* $\forall\exists$.

Préservation par produit réduit

5.10 On va maintenant franchir un nouveau cap et s'intéresser à la préservation par produit réduit.

DEFINITION 1 : *Les* ***formules de Horn élémentaires*** *sont les formules de la forme :*

$$H_1 \vee H_2 \vee \ldots \vee H_n$$

où l'une au plus des formules H_i *(pour* i *compris entre 1 et* n*) est une formule atomique, les autres étant des négations de formules atomiques.*

Une ***formule de Horn*** *est une formule que l'on peut obtenir à partir de formules de Horn élémentaires en utilisant la conjonction et les quantifications existentielles et universelles.*

Les formules de Horn élémentaires sont des clauses (voir la définition 5.6 du chapitre 4). A équivalence logique près, les formules de Horn élémentaires sont donc les formules d'une des deux formes suivantes :

- $(F_1 \wedge F_2 \wedge \ldots \wedge F_{n-1}) \Longrightarrow F_n$, où, pour k compris entre 1 et n, les F_k sont des formules atomiques ; c'est le cas où il y a effectivement une formule atomique parmi les formules H_k de la définition ;
- $H_1 \vee H_2 \vee \ldots \vee H_n$ où toutes les H_k, pour k compris entre 1 et n sont des négations de formules atomiques. On pourrait écrire ces formules sous la forme précédente si on admet la formule toujours fausse parmi les formules atomiques.

Par définition, la conjonction d'un nombre fini de formules de Horn est encore une formule de Horn. On voit facilement qu'une formule de Horn est équivalente à une formule de la forme :

$$Q_1 v_1 Q_2 v_2 \ldots Q_n v_n (G_1 \wedge G_2 \wedge \ldots \wedge G_k)$$

où chaque Q_i, pour i compris entre 1 et n, représente le quantificateur $\forall$ ou le quantificateur $\exists$, et les G_j, pour j compris entre 1 et k sont des formules de Horn élémentaires.

EXEMPLE : La théorie des groupes et celle des anneaux s'axiomatisent à l'aide de formules de Horn. En revanche, on peut voir (exercice 14), qu'il est impossible d'axiomatiser la théorie des corps par des formules de Horn. C'est l'axiome :

$$\forall v_1 \exists v_2 (\neg v_1 \simeq 0 \Rightarrow v_1 \cdot v_2 \simeq 1)$$

qui n'est pas équivalent à une formule de Horn.

DEFINITION 2 : *On dit qu'une formule close* F *d'un langage* L *est* ***préservée par produit réduit*** *si, pout tout ensemble* I, *pour tout filtre* $\mathcal{F}$ *sur* I, *et toute famille* $(\mathfrak{M}_i \,;\, i \in I)$ *de* L*-structures, si* $\{i \in I \,;\, \mathfrak{M}_i \models F\} \in \mathcal{F}$, *alors*

$$\prod_{i \in I} \mathfrak{M}_i / \mathcal{F} \models F.$$

5.11 PROPOSITION : *Les formules de Horn sont préservées par produit réduit.*

☺ La proposition découle de la propriété suivante :

(*) Pour toute formule de Horn $G[v_1,v_2,\ldots,v_n]$ de L, pour toute famille $(\mathfrak{M}_i \,;\, i \in I)$ de L-structures, pour tout filtre $\mathcal{F}$ sur I et pour tous $a_1,a_2,\ldots,a_n$ de $\prod_{i \in I} M_i$,

si $\{i \in I \,;\, \mathfrak{M}_i \models G[a_1^i,a_2^i,\ldots,a_n^i]\} \in \mathcal{F}$ alors $\prod_{i \in I} \mathfrak{M}_i / \mathcal{F} \models G[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n]$.

(On reprend ici les notations de la section 4 : si $a \in \prod_{i \in I} M_i$, a^i est la i-ème coordonnée de a et $\bar{a}$ est la classe de a relativement à $\approx_{\mathcal{F}}$).

On va montrer (*) par récurrence sur le nombre d'étapes nécessaires pour obtenir $G[v_1,v_2,\ldots,v_n]$ à partir de formules de Horn élémentaires.

• Cas où $G[v_1,v_2,\ldots,v_n]$ est une formule de Horn élémentaire : on peut alors écrire $G[v_1,v_2,\ldots,v_n]$ sous la forme $H_1[v_1,v_2,\ldots,v_n] \vee H_2[v_1,v_2,\ldots,v_n] \vee \ldots \vee H_k[v_1,v_2,\ldots,v_n]$ où H_1 est soit une formule atomique, soit une formule toujours fausse, et où, pour j compris entre 2 et k, $H_j = \neg J_j$, où J_j est une formule atomique.

Posons, pour chaque j compris entre 1 et k, $X_j = \{i \in I \,;\, \mathfrak{M}_i \models H_j[a_1^i,a_2^i,\ldots,a_n^i]\}$ et appelons Y_j le complémentaire de X_j dans I. Par hypothèse :

$$\bigcup_{1 \leqslant j \leqslant k} X_j = \{i \in I \,;\, \mathfrak{M}_i \models G[a_1^i,a_2^i,\ldots,a_n^i]\} \in \mathcal{F}.$$

On distingue deux possibilités.

- Première possibilité : il existe un entier j compris entre 2 et k tel que Y_j n'appartienne pas à $\mathcal{F}$. Cela veut dire que $\{i \in I \,;\, \mathfrak{M}_i \models J_j[a_1^i,a_2^i,\ldots,a_n^i]\} \notin \mathcal{F}$; par définition du produit réduit et parce que J_j est atomique, cela implique que $\prod_{i \in I} \mathfrak{M}_i / \mathcal{F} \not\models J_j[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n]$, donc que :

$$\prod_{i \in I} \mathfrak{M}_i/\mathcal{F} \vDash G[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n].$$

- Dans le cas contraire, $\bigcap_{2<j<k} Y_j \in \mathcal{F}$. Mais :

$$[\bigcup_{1<j<k} X_j] \cap [\bigcap_{2<j<k} Y_j] \subseteq X_1 ,$$

et ceci implique que $X_1 = \{i \in I ; \mathfrak{M}_i \vDash H_1[a_1^i,a_2^i,\ldots,a_n^i]\} \in \mathcal{F}$; dans ce cas, H_1 est une formule atomique (sinon, l'ensemble vide appartiendrait à $\mathcal{F}$), et, d'après la définition du produit réduit, $\prod_{i \in I} \mathfrak{M}_i/\mathcal{F} \vDash H_1[\bar{a}_1,\bar{a}_2,\ldots ,\bar{a}_n]$, et donc $\prod_{i \in I} \mathfrak{M}_i/\mathcal{F} \vDash G[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n]$.

• Cas où $G = G_1 \wedge G_2$: il n'y a guère de problème : si

$\{i \in I ; \mathfrak{M}_i \vDash G[a_1^i,a_2^i,\ldots,a_n^i]\} \in \mathcal{F}$,

alors $\{i \in I ; \mathfrak{M}_i \vDash G_1[a_1^i,a_2^i,\ldots,a_n^i]\} \in \mathcal{F}$ et $\{i \in I ; \mathfrak{M}_i \vDash G_2[a_1^i,a_2^i,\ldots,a_n^i]\} \in \mathcal{F}$,

et, par hypothèse d'induction,

$$\prod_{i \in I} \mathfrak{M}_i/\mathcal{F} \vDash G_1[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n] \text{ et } \prod_{i \in I} \mathfrak{M}_i/\mathcal{F} \vDash G_2[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n],$$

donc $\prod_{i \in I} \mathfrak{M}_i/\mathcal{F} \vDash G_1[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n] \wedge G_2[\bar{a}_1,\bar{a}_2,\ldots,\bar{a}_n]$.

• Cas où $G = \exists v_0 G_1[v_0,v_1,\ldots,v_n]$: si l'ensemble $X = \{i \in I ; \mathfrak{M}_i \vDash G[a_1^i,a_2^i,\ldots,a_n^i]\}$ appartient à $\mathcal{F}$ on peut définir un élément $a_0 \in \prod_{i \in I} M_i$ de la façon suivante : si $i \in X$, a_0^i est un point de M_i tel que :

$$\mathfrak{M}_i \vDash G_1[a_0^i,a_1^i,\ldots,a_n^i] ;$$

si $i \notin X$, on prend pour a_0^i n'importe quel point de M_i ; on voit alors que :

$\{i \in I ; \mathfrak{M}_i \vDash G_1[a_0^i,a_1^i,\ldots,a_n^i]\} = X$,

et, par hypothèse d'induction,

$$\prod_{i \in I} \mathfrak{M}_i/\mathcal{F} \vDash G_1[\bar{a}_0,\bar{a}_1,\ldots,\bar{a}_n]$$

et donc $\prod_{i \in I} \mathfrak{M}_i/\mathcal{F} \vDash G[\bar{a}_1,\ldots,\bar{a}_n]$.

• Cas où $G = \forall v_0 G_1[v_0,v_1,\ldots,v_n]$: notre hypothèse est que :

$$X = \{i \in I ; \mathfrak{M}_i \vDash \forall v_0 G_1[v_0,a_1^i,a_2^i,\ldots,a_n^i]\} \in \mathcal{F} ;$$

soit $a_0 \in \prod_{i \in I} M_i$; on veut montrer que $\prod_{i \in I} \mathfrak{M}_i/\mathcal{F} \vDash G_1[\bar{a}_0,\bar{a}_1,\ldots,\bar{a}_n]$. Or pour tout $i \in X$, $\mathfrak{M}_i \vDash G_1[a_0^i,a_1^i,\ldots,a_n^i]$, donc l'ensemble $\{ i ; \mathfrak{M}_i \vDash G_1[a_0^i,a_1^i,\ldots,a_n^i] \}$ contient X et appartient à $\mathcal{F}$. Par hypothèse d'induction, cela implique que :

$$\prod_{i \in I} \mathfrak{M}_i/\mathcal{F} \vDash G_1[\bar{a}_0,\bar{a}_1,\ldots,\bar{a}_n].$$

☺

5.12 La réciproque de cette proposition est vraie : toute formule qui est préservée par produit réduit est équivalente à une formule de Horn. Cependant, la démonstration utilise des techniques qui n'ont pas été abordées dans ce court aperçu et on ne la donnera pas ici. On se contentera des formules de Horn universelles.

PROPOSITION : *Soit* F *une formule close. Les trois conditions suivantes sont équivalentes :*

i) F *est équivalente à une formule de Horn universelle ;*

ii) F *est préservée par produit réduit et par sous-structure ;*

iii) F *est préservée par produit fini et par sous-structure.*

☺ L'implication *i)* $\Longrightarrow$ *ii)* découle de la proposition 5.11 et du corollaire 5.3 ; L'implication *ii)* $\Longrightarrow$ *iii)* est évidente. Voyons l'implication *iii)* $\Longrightarrow$ *i)*. Puisque F est préservée par sous-structure, elle est équivalente à une formule universelle :

$$G = \forall v_1 \forall v_2 \ldots \forall v_n H[v_1, v_2, \ldots, v_n].$$

On peut de plus supposer que H est écrite sous forme conjonctive, (voir chapitre 3, 4.3), c'est-à-dire :

$$H[v_1,v_2,\ldots,v_n] = H_1[v_1,v_2,\ldots,v_n] \wedge H_2[v_1,v_2,\ldots,v_n] \wedge \ldots \wedge H_k[v_1,v_2,\ldots,v_n],$$

où chacune des formules H_i, pour i compris entre 1 et k, est la disjonction de formules atomiques et de négations de formules atomiques. Or les quantificateurs universels commutent avec la conjonction, ce qui fait que notre formule G est équivalente à l'ensemble suivant :

$$\{ \forall v_1 \forall v_2 \ldots \forall v_n H_i[v_1,v_2,\ldots,v_n] \; ; \; 1 \leqslant i \leqslant k \}.$$

On va remplacer chacune des formules $\forall v_1 \forall v_2 \ldots \forall v_n H_i[v_1,v_2,\ldots,v_n]$ par une formule de Horn grâce au lemme suivant :

LEMME : *Soient* T *une théorie,* K *une formule close de la forme :*

$$\forall v_1 \forall v_2 \ldots \forall v_n (A_1 \vee A_2 \vee \ldots \vee A_u \vee \neg B_1 \vee \neg B_2 \vee \ldots \vee \neg B_t),$$

où chaque A_i, *pour* i *compris entre* 1 *et* u *est une formule atomique, de même que chaque* B_j, *pour* j *compris entre* 1 *et* t. *On suppose que* $T \cup \{K\}$ *est préservée par produit fini. Alors il existe une formule de Horn universelle* J *telle que :*

$$T \vdash K \Longleftrightarrow J .$$

☺ Pour chaque v compris entre 1 et u, considérons la formule :

$$K_v = \forall v_1 \forall v_2 \ldots \forall v_n (A_v \vee \neg B_1 \vee \neg B_2 \vee \ldots \vee \neg B_t).$$

C'est manifestement une formule de Horn universelle ; il est tout aussi manifeste que $\vdash K_v \Longrightarrow K$. On va montrer qu'il existe un entier v compris entre 1 et u tel que :

$$T \vdash K \Longrightarrow K_v .$$

On raisonne par l'absurde et on suppose le contraire : pour $1 \leqslant v \leqslant u$, on obtient une structure $\mathfrak{M}_v$ qui est modèle de T, de K et de $\neg K_v$. Il existe donc dans M_v des points $a_1^v, a_2^v, \ldots, a_n^v$ tels que :

$\mathfrak{M}_v \models \neg A_v[a_1^v, a_2^v, \ldots, a_n^v]$ et $\mathfrak{M}_v \models B_i[a_1^v, a_2^v, \ldots, a_n^v]$ pour $1 \leqslant i \leqslant t$.

Considérons alors le produit $\mathfrak{M} = \prod_{1 \leqslant i \leqslant u} \mathfrak{M}_i$, et, dans ce produit, les points $a_k = (a_k^v \,;\, 1 \leqslant v \leqslant u)$ pour $1 \leqslant k \leqslant n$. Par définition du produit, on a :

$\mathfrak{M} \models \neg A_v[a_1, a_2, \ldots, a_n]$ pour v compris entre 1 et u,

et $\mathfrak{M} \models B_v[a_1, a_2, \ldots, a_n]$ pour v compris entre 1 et t.

On en déduit que K n'est pas satisfaite dans $\mathfrak{M}$, ce qui contredit le fait que $T \cup \{K\}$ est préservée par produit fini.

☺

Revenons à la preuve de la proposition : on applique le lemme à la formule $K = \forall v_1 \forall v_2 \ldots \forall v_n H_1[v_1, v_2, \ldots, v_n]$ et à la théorie $T = \{\forall v_1 \forall v_2 \ldots \forall v_n H_i[v_1, v_2, \ldots, v_n] \,;\, 2 \leqslant i \leqslant k\}$. On obtient une formule de Horn universelle J_1, de telle sorte que G soit équivalente à l'ensemble

$$\{J_1\} \cup \{\forall v_1 \forall v_2 \ldots \forall v_n H_i[v_1, v_2, \ldots, v_n] \,;\, 2 \leqslant i \leqslant k\}.$$

puis on fait la même chose pour remplacer la formule $\forall v_1 \forall v_2 \ldots \forall v_n H_2[v_1, v_2, \ldots, v_n]$ par une formule de Horn universelle, etc., jusqu'à obtenir une ensemble de formules de Horn universelles, qui lui-même est équivalent à une formule de Horn universelle.

☺

6. LES THEORIES ALEPH-ZERO CATEGORIQUES

Le théorème d'omission des types

6.1 Rappelons qu'une théorie $\aleph_0$-catégorique est une théorie ayant un modèle dénombrable, et dont tous les modèles dénombrables sont isomorphes. Les modèles dénombrables d'une telle théorie possèdent un certain nombre de belles propriétés que nous allons mettre en évidence. Dans toute cette section, T sera une théorie complète dans un langage L dénombrable, et modèle voudra dire : modèle de T. On commence par introduire les notions de types et de types isolés, qui sont essentielles dans cette matière.

DEFINITIONS :

1°) Soit n *un entier. Un* **n-type** p *est un ensemble de formules de* L, *clos par conjonction et tel que seules les variables* v_0, v_1, ..., v_{n-1} *peuvent être libres dans une formule de* p. *On parlera de* **type** *si on ne veut pas préciser la valeur de l'entier* n.

2°) Soient p *un* n*-type,* $\mathfrak{M}$ *un modèle et* $a_0,a_1,...,a_{n-1}$ *des points de* $\mathfrak{M}$. *On dit que la suite* $(a_0,a_1,...,a_{n-1})$ ***réalise*** p *si, pour toute formule* $F[v_0,v_1,...,v_{n-1}]$ *de* p, *on a :*

$$\mathfrak{M} \models F[a_0,a_1,...,a_{n-1}].$$

3°) On dit qu'un modèle $\mathfrak{M}$ ***réalise*** *un* n*-type* p, *ou que* p ***est réalisé dans*** $\mathfrak{M}$, *s'il existe une suite de* $\mathfrak{M}$ *réalisant* p. *Dans le cas contraire, on dit que* $\mathfrak{M}$ ***omet*** p.

4°) Soit $\bar{a} = (a_0,a_1,...,a_{n-1})$ *une suite de points d'un modèle* $\mathfrak{M}$. *On appelle* ***type de*** $\bar{a}$ ***dans*** $\mathfrak{M}$, *et on note* $t(\bar{a}/\mathfrak{M})$ *le* n*-type :*

$$\{ F[v_0,v_1,...,v_{n-1}] \; ; \; \mathfrak{M} \models F[a_0,a_1,...,a_{n-1}] \}.$$

5°) Soient p *un* n*-type et* $G[v_0,v_1,...,v_{n-1}]$ *une formule. On dit que* $G[v_0,v_1,...,v_{n-1}]$ ***isole*** p *si :*

$$T \vdash \exists v_0 \exists v_1 ... \exists v_{n-1} G[v_0,v_1,...,v_{n-1}],$$

et, pour toute formule $F[v_0,v_1,...,v_{n-1}]$ *de* p :

$$T \vdash \forall v_0 \forall v_1 ... \forall v_{n-1} (G[v_0,v_1,...,v_{n-1}] \Longrightarrow F[v_0,v_1,...,v_{n-1}]).$$

On dit que p ***est isolé*** *s'il existe une formule qui l'isole.*

6.2 Voici d'abord quelques lemmes et remarques avant d'aborder le théorème clef qui est le théorème d'omission des types.

LEMME 1 : *Si* p *est un* n*-type, alors les trois conditions suivantes sont équivalentes :*

i) *il existe un modèle dénombrable réalisant* p ;

ii) *il existe un modèle réalisant* p ;

iii) *pour toute formule* $F[v_0,v_1,...,v_{n-1}] \in p$, *on a :*

$$T \vdash \exists v_0 \exists v_1 ... \exists v_{n-1} F[v_0,v_1,...,v_{n-1}].$$

☺ Il est évident que la condition *i)* implique la condition *ii)*. Montrons que cette dernière implique *iii)*. Si $\mathfrak{M}$ est un modèle de T et $(a_0,a_1,...,a_{n-1})$ une suite de points de M réalisant p et $F[v_0,v_1,...,v_{n-1}] \in p$,, alors,

$$\mathfrak{M} \models F[a_0,v_1,...,a_{n-1}],$$

et donc : $\mathfrak{M} \models \exists v_0 \exists v_1 ... \exists v_{n-1} F[v_0,v_1,...,v_{n-1}]$.

Puisque T est complète, tout autre modèle de T est élémentairement équivalent à $\mathfrak{M}$, et par conséquent :

$$T \vdash \exists v_0 \exists v_1 \ldots \exists v_{n-1} F[v_0,v_1,\ldots,v_{n-1}].$$

Supposons maintenant que la condition *iii)* soit vérifiée. Ajoutons au langage L des symboles de constante, c_0, c_1, ...,c_{n-1}, et considérons la théorie T' suivante :

$$T' = T \cup \{ F[c_0,c_1,\ldots,c_{n-1}] \; ; \; F[v_0,v_1,\ldots,v_{n-1}] \in p \}.$$

Cette théorie est consistante : sinon, par le théorème de compacité, il existerait un sous-ensemble fini p_0 de p tel que :

$$T \cup \{ F[c_0,c_1,\ldots,c_{n-1}] \; ; \; F[v_0,v_1,\ldots,v_{n-1}] \in p_0 \}$$

soit inconsistante. La conjonction $G[v_0,v_1,\ldots,v_{n-1}]$ des formules de p_0 appartient à p (parce que p est clos par conjonction) et :

$$T \vdash \neg G[c_0,c_1,\ldots,c_{n-1}].$$

Comme les symboles c_0, c_1, ...,c_{n-1} n'apparaissent pas dans T, on en déduit, comme d'habitude, que :

$$T \vdash \neg \exists v_0 \exists v_1 \ldots \exists v_{n-1} G[v_0,v_1,\ldots,v_{n-1}],$$

ce qui contredit *iii)*.

Par le théorème de Löwenheim-Skolem, on peut trouver un modèle dénombrable $\mathfrak{M}'$ de T'. Si, pour i compris entre 0 et n – 1, on appelle a_i le point de ce modèle qui interprète c_i, et si on appelle $\mathfrak{M}$ le réduit de $\mathfrak{M}'$ au langage originel L, alors la suite $(a_0,a_1,\ldots,a_{n-1})$ réalise le type p dans $\mathfrak{M}$.

☺

DEFINITION : *On dit qu'un* **type est consistant** *s'il satisfait les conditions du lemme 1.*

Les deux remarques suivantes sont évidentes :

REMARQUE 1 : Si $\mathfrak{M}' \prec \mathfrak{M}$ et si la suite $(a_0,a_1,\ldots,a_{n-1})$ réalise le type p dans $\mathfrak{M}'$, alors cette même suite réalise p dans $\mathfrak{M}$.

REMARQUE 2 : Si $\mathfrak{M}$ et $\mathfrak{M}'$ sont deux modèles isomorphes et si p est réalisé dans l'un de ces deux modèles, alors il est réalisé dans l'autre.

LEMME 2 : *Soient* p *un type consistant et* $\mathfrak{M}$ *un modèle. Alors il existe une extension élémentaire* $\mathfrak{M}_1$ *de* $\mathfrak{M}$ *dans laquelle* p *est réalisé.*

☹ On sait qu'il existe un modèle $\mathfrak{M}'$ dans lequel p est réalisé. Comme $\mathfrak{M}$ et $\mathfrak{M}'$ sont élémentairement équivalents, il existe une extension élémentaire $\mathfrak{M}_1$ de $\mathfrak{M}$ et un plongement élémentaire de $\mathfrak{M}'$ dans $\mathfrak{M}_1$ (théorème 3.1), donc une sous-structure élémentaire $\mathfrak{M}_2$ de $\mathfrak{M}_1$ isomorphe à $\mathfrak{M}'$. Les remarques 1 et 2 montrent que p est réalisé dans $\mathfrak{M}_1$.
☺

REMARQUE 3 : Un type isolé est réalisé dans tout modèle de T (et est donc consistant).

Soit p un n-type isolé, et soit $G[v_0,v_1,\ldots,v_{n-1}]$ une formule qui l'isole. Si $\mathfrak{M}$ est un modèle de T, il existe dans M des points a_0, a_1, ...,a_{n-1} tels que :

$$\mathfrak{M} \models G[a_0,a_1,\ldots,a_{n-1}].$$

Il est alors clair que le suite $(a_0,a_1,\ldots,a_{n-1})$ réalise p.

6.3 **Le théorème d'omission des types** est une réciproque à la remarque 3.

THEOREME : *Soit* p *un* n*-type non isolé. Alors il existe un modèle dénombrable de* T *omettant* p.

☹ On va construire un modèle de T en utilisant la méthode de Henkin qui nous a permis, au chapitre 4, de démontrer le théorème de complétude. Pour obtenir un modèle omettant p, il va falloir jouer un peu plus serré.

Soit $C = \{c_i ; i \in \omega\}$ un ensemble infini de nouveaux symboles de constante que l'on adjoint à L pour obtenir L'. On va construire une théorie T' dans L' jouissant des propriétés suivantes :

1°) $T \subseteq T'$;

2°) T' est complète dans L' ;

3°) T' admet des témoins de Henkin : si $F[v_0]$ est une formule de L', alors il existe un entier i tel que $\exists v_0 F[v_0] \Rightarrow F[c_i] \in T'$;

4°) si $(d_0,d_1,\ldots,d_{n-1})$ est une suite de longueur n d'éléments de C, alors il existe une formule $F[v_0,v_1,\ldots,v_{n-1}] \in p$ tel que :

$$\neg F[d_0,d_1,\ldots,d_{n-1}] \in T'.$$

Il est conseillé au lecteur de relire les démonstrations des propositions A et B se trouvant en 2.3 et 2.4 du chapitre 4. On y retrouve les conditions 1°), 2°) et 3°) ci-dessus, et, à l'aide de ces conditions, on montre les propriétés suivantes :

- la relation binaire R sur C définie par :

pour tous i et j dans ω, $R(c_i,c_j)$ si et seulement si $T' \vdash c_i \simeq c_j$

est une relation d'équivalence ; si $d \in C$, on notera $\bar{d}$ sa classe modulo R ;

• appelons M l'ensemble des classes d'équivalence relativement à cette relation ; alors on peut définir une L'-structure $\mathfrak{M}'$ dont l'ensemble de base est M et telle que :

(*) pour tout entier n, pour tous symboles d_0, d_1, ..., d_{n-1} de C, pour toute formule $F[v_0,v_1,...,v_{n-1}]$ de L' : $\mathfrak{M}' \models F[\bar{d}_0,\bar{d}_1,...,\bar{d}_{n-1}]$ si et seulement si $F[d_0,d_1,...,d_{n-1}] \in T'$.

On utilise maintenant la condition 4°) pour montrer que $\mathfrak{M}$, le réduit de $\mathfrak{M}'$ à L, omet le type p : soit $(a_0,a_1,...,a_{n-1})$ une suite de points de M, et, pour chaque i compris entre 0 et n − 1, d_i un point de C tel que a_i soit la classe de d_i. On sait, par 4°), qu'il existe une formule $F[v_0,v_1,...,v_{n-1}] \in p$ telle que $\neg F[d_0,d_1,...,d_{n-1}] \in T'$, et on en déduit, par (*), que $\mathfrak{M} \models \neg F[a_0,a_1,...,a_{n-1}]$: aucune suite de M ne réalise p.

Petite digression : le lecteur qui répugnerait à se replonger dans la démonstration du théorème de complétude peut remplacer le raisonnement ci-dessus (comment construire un modèle omettant p à partir de T') par l'argument suivant : T' est une théorie consistante, donc admet un modèle $\mathfrak{M}'$; si on appelle N le sous-ensemble de $\mathfrak{M}'$ des interprétations de C, alors on voit au moyen de la condition 3°), du test de Tarski-Vaught (théorème 1.4) et de la remarque qui l'accompagne, que N est l'ensemble de base d'une sous-structure élémentaire $\mathfrak{N}$ de $\mathfrak{M}'$; le réduit de $\mathfrak{N}$ au langage L est donc un modèle de T, et on vérifie, au moyen de la condition 4°), qu'il omet p.

Reste à construire T'. Pour ce faire, on aura besoin :

• d'une énumération $(K_i\, ;\, i \in \mathbb{N})$ de toutes les formules closes de L' ;

• d'une énumération $(G_i[v_0]\, ;\, i \in \mathbb{N})$ de toutes les formules de L' à une seule variable libre v_0 ;

• d'une énumération $(\gamma_i\, ;\, i \in \mathbb{N})$ de toutes les suites de C de longueur n.

On définit par récurrence sur l'entier k une suite de théories $(T_k\, ;\, k \in \mathbb{N})$ qui, entre autres, satisfera les propriétés suivantes :

- pour tout $k \in \mathbb{N}$, T_k est l'union de T et d'un ensemble fini de formules closes de L' ;

- pour tout $k \in \mathbb{N}$, T_k est une théorie consistante ;

- pour tous k, $m \in \mathbb{N}$, si $k \leqslant m$, alors $T_k \subseteq T_m$.

La théorie T' sera l'union des théories T_k, pour $k \in \mathbb{N}$, et on voit déjà que ce sera une théorie consistante contenant T.

On commence la récurrence avec $T_0 = T$.

Soit k un entier positif ou nul. On suppose que T_m a déjà été défini pour tout $m \leqslant k$. La définition de T_{k+1} se scinde en trois cas, suivant que k est congru à 0, 1 ou 2 modulo 3.

• Cas où $k = 3i$, pour un entier i : si $T_k \cup \{K_i\}$ est une théorie consistante, alors on pose $T_{k+1} = T_k \cup \{K_i\}$; sinon, comme T_k est consistante par hypothèse d'induction, c'est que $T_k \cup \{\neg K_i\}$ est consistante, et on pose $T_{k+1} = T_k \cup \{\neg K_i\}$.

• Cas où $k = 3i + 1$, pour un entier i : on choisit un entier j tel que c_j n'apparaisse ni dans T_k, ni dans G_i (c'est possible puisque T_k est l'union de T, où aucune constante de C n'a d'occurrence, et d'un ensemble fini de formules). On pose :

$$T_{k+1} = T_k \cup \{\exists v_0 G_i[v_0] \Rightarrow G_i[c_j]\}.$$

La théorie T_{k+1} est consistante par le lemme 2.4 du chapitre 4.

Pour l'instant, on n'a fait que copier la démonstration du théorème de complétude, en laissant libre une étape sur 3. On est déjà assuré que la théorie T' sera complète et admettra des témoins de Henkin.

• Cas où $k = 3i + 2$, pour un entier i : soient $d_0, d_1, \ldots, d_{n-1}$ des symboles de C tels que $\gamma_i = (d_0, d_1, \ldots, d_{n-1})$. On sait, par hypothèse de récurrence qu'il existe une formule close H de L' telle que T_k est équivalente à $T \cup \{H\}$. On peut écrire H sous la forme

$$H = D[d_0, d_1, \ldots, d_{n-1}, e_0, e_1, \ldots, e_{m-1}]$$

où $D[v_0, v_1, \ldots, v_{n-1}, v_n, v_{n+1}, \ldots, v_{n+m-1}]$ est une formule de L, et où, pour tout i compris entre 0 et $n - 1$ et pour tout j compris entre 0 et $m - 1$, $e_j \in C$ et $d_i \neq e_j$. Posons :

$$E[v_0, v_1, \ldots, v_{n-1}] = \exists v_n \exists v_{n+1} \ldots \exists v_{n+m-1} D[v_0, v_1, \ldots, v_{n-1}, v_n, v_{n+1}, \ldots, v_{n+m-1}].$$

La formule $\exists v_0 \exists v_1 \ldots \exists v_{n-1} E[v_0, v_1, \ldots, v_{n-1}]$ est conséquence de T_k. Comme c'est une formule close de L et comme T est complète, on a :

$$T \vdash \exists v_0 \exists v_1 \ldots \exists v_{n-1} E[v_0, v_1, \ldots, v_{n-1}].$$

Parce que p n'est pas un type isolé, il contient une formule $F[v_0, v_1, \ldots, v_{n-1}]$ telle que :

$$T \cup \{\neg(\forall v_0 \forall v_1 \ldots \forall v_{n-1}(E[v_0, v_1, \ldots, v_{n-1}] \Rightarrow F[v_0, v_1, \ldots, v_{n-1}]))\}$$

soit consistante. Cela revient à dire que :

$$T \cup \{\exists v_0 \exists v_1 \ldots \exists v_{n-1}(\exists v_n \exists v_{n+1} \ldots \exists v_{n+m-1} D[v_0, v_1, \ldots, v_{n-1}, v_n, v_{n+1}, \ldots, v_{n+m-1}] \wedge \neg F[v_0, v_1, \ldots, v_{n-1}]\}$$

est consistante, ou encore que la théorie :

$$T \cup \{\exists v_0 \exists v_1 \ldots \exists v_{n+m-1}(D[v_0, v_1, \ldots, v_{n-1}, v_n, v_{n+1}, \ldots, v_{n+m-1}] \wedge \neg F[v_0, v_1, \ldots, v_{n-1}])\}$$

est consistante. Puisque les constantes de C n'apparaissent pas dans cette théorie, on en déduit, toujours à l'aide du lemme 2.4 de chapitre 4, que

$$T \cup \{D[d_0, d_1, \ldots, d_{n-1}, e_0, e_1, \ldots, e_{m-1}] \wedge \neg F[d_0, d_1, \ldots, d_{n-1}]\}$$

est une théorie consistante. Il suffit donc de poser :

$$T_{k+1} = T_k \cup \{\neg F[d_0, d_1, \ldots, d_{n-1}]\}.$$

☺

6.4 REMARQUE : On peut modifier la démonstration précédente et obtenir le résultat plus fort suivant : soit $\{p_j \,;\, j \in \mathbb{N}\}$ un ensemble dénombrable de types non isolés (pour fixer les idées, disons que p_j est un n_j-type). Alors il existe un modèle dénombrable de T ne réalisant aucun des types p_j, pour $j \in \mathbb{N}$.

Il sufffit, dans la démonstration précédente de mieux tirer parti des étapes de la forme $3i+2$: on énumère l'ensemble des couples (γ,j), où γ est une suite finie de C, j est un entier et la longueur de γ est égale à n_j. En utilisant la même technique de sabotage que ci-dessus (celle qui nous a permis, à l'étape $3i+2$ de la preuve ci-dessus d'empêcher que la suite γ_i ne réalise le type p en exigeant que cette suite satisfasse le négation d'une formule de p), on s'assure à l'étape $3i+2$ que, si (γ,j) est le couple numéro i, alors γ ne réalise pas p_j.

Structures aleph-zéro-catégoriques

6.5 COROLLAIRE 1 : *Supposons que* T *soit une théorie* $\aleph_0$*-catégorique. Alors tout type consistant est isolé.*

☹ Supposons qu'il existe un type p non isolé et consistant. D'après la définition 2.1, il existe un modèle dénombrable réalisant p. Le théorème 6.4 affirme, lui, qu'il existe un modèle dénombrable omettant p. Ces deux modèles ne peuvent pas être isomorphes (remarque 2 de 6.2), et T n'est pas $\aleph_0$-catégorique.
☺

DEFINITION : *On dit qu'un* n-***type*** p ***est complet****, si, premièrement il est consistant, et deuxièmement, pour toute formule* $F[v_0,v_1,\ldots,v_{n-1}]$ *de* L, $F[v_0,v_1,\ldots,v_{n-1}] \in p$ ou $\neg F[v_0,v_1,\ldots,v_{n-1}] \in p$. *On notera* S_n *l'ensemble des* n-*types complets.*

On remarque que si p et q sont deux n-types complets et si $p \subseteq q$, alors $p = q$: en effet, si $F[v_0,v_1,\ldots,v_{n-1}] \notin p$, alors $\neg F[v_0,v_1,\ldots,v_{n-1}] \in p$, donc $\neg F[v_0,v_1,\ldots,v_{n-1}] \in q$, et, puisque q est consistant, $F[v_0,v_1,\ldots,v_{n-1}] \notin q$.

Par exemple, si $\bar{a}$ est une suite de longueur n d'un modèle $\mathfrak{M}$, $t(\bar{a}/\mathfrak{M})$ est un type complet. Réciproquement, si p est un n-type complet, alors il existe un modèle $\mathfrak{M}$, que l'on peut même supposer dénombrable, et une suite $\bar{a}$ de $\mathfrak{M}$ réalisant p, et on voit sans peine que $t(\bar{a}/\mathfrak{M}) = p$.

COROLLAIRE 2 : *Supposons que* T *soit une théorie* $\aleph_0$*-catégorique. Alors, pour tout entier* n, *l'ensemble* S_n *est fini.*

☹ Si p est un n-type complet, il est isolé (corollaire 1) ; choisissons une formule $F_p[v_0,v_1,\ldots,v_{n-1}]$ qui l'isole. Puisque

$$T \vdash \exists v_0 \exists v_1 \ldots \exists v_{n-1} F_p[v_0,v_1,\ldots,v_{n-1}],$$

il est faux que :

$$T \vdash \forall v_0 \forall v_1 \ldots \forall v_{n-1}(F_p[v_0,v_1,\ldots,v_{n-1}] \Rightarrow \neg F_p[v_0,v_1,\ldots,v_{n-1}]) ;$$

donc $\neg F_p[v_0,v_1,\ldots,v_{n-1}]$ n'appartient pas à p. Comme p est complet, $F_p[v_0,v_1,\ldots,v_{n-1}]$ appartient à p.

Si p et q sont deux n-types complets distincts, alors $\neg F_p \in q$: supposons le contraire en vue d'obtenir une contradiction ; parce que q est complet, on a : $F_p \in q$. Si $F[v_0,v_1,\ldots,v_{n-1}] \in p$, alors, par choix de F_p, $\neg F[v_0,v_1,\ldots,v_{n-1}] \wedge F_p[v_0,v_1,\ldots,v_{n-1}]$ n'est pas consistant, et donc $\neg F[v_0,v_1,\ldots,v_{n-1}] \notin q$. Comme q est complet, on en déduit que $F[v_0,v_1,\ldots,v_{n-1}] \in q$: on a montré que $p \subseteq q$, et on a déjà remarqué que cela impliquait que $p = q$.

Raisonnons encore par l'absurde et supposons que, pour un entier n, l'ensemble S_n soit infini. Ajoutons au langage un ensemble $\{c_i \,;\, 0 \leqslant i \leqslant n-1\}$ de nouveaux symboles de constante deux à deux distincts, et considérons la théorie :

$$T' = T \cup \{\neg F_p[c_0,c_1,\ldots,c_{n-1}] \,;\, p \in S_n\}.$$

Cette théorie est consistante. Pour le prouver, il suffit, en vertu du théorème de compacité, de montrer que, pour tout sous-ensemble fini X de S_n, la théorie :

$$T_X = T \cup \{\neg F_p[c_0,c_1,\ldots,c_{n-1}] \,;\, p \in X\}$$

est consistante. Choisissons un n-type complet q n'appartenant pas à X (c'est possible car X est fini et il y a une infinité de n-types complets), un modèle $\mathfrak{M}$ et une suite $(a_0,a_1,\ldots,a_{n-1})$ de points de M telle que $t((a_0,a_1,\ldots,a_{n-1})/\mathfrak{M}) = q$. On a vu que, pour tout $p \in X$, $\neg F_p \in q$, et donc :

$$\mathfrak{M} \models \neg F_p[a_0,a_1,\ldots,a_{n-1}].$$

Pour avoir un modèle de T_X, il suffit d'interpréter c_i par a_i, pour i compris entre 0 et $n - 1$.

Il existe donc un modèle $\mathfrak{M}$ de T' contenant des points b_0, b_1, ..., b_{n-1} tels que, pour tout $p \in S_n$, $\mathfrak{M} \models \neg F_p[b_0,b_1,\ldots,b_{n-1}]$. Alors $t((b_0,b_1,\ldots,b_{n-1})/\mathfrak{M})$ ne peut pas appartenir à S_n, ce qui constitue une contradiction.
☺

6.6 On va montrer une réciproque au corollaire 1 de 6.5.

THEOREME : *Supposons que, pour tout entier* n, *tout* n*-type complet soit isolé ; alors* T *est* $\aleph_0$*-catégorique.*

☹ On montre d'abord deux lemmes :

LEMME 1 : *On suppose que, pour tout entier* n, *tout* n*-type complet est isolé. Soient* $\mathfrak{M}$ *et* $\mathfrak{N}$ *deux modèles de* T, $(a_0,a_1,\dots,a_{n-1})$ *et* $(b_0,b_1,\dots,b_{n-1})$ *des suites de* M *et* N, *respectivement telles que* $t((a_0,a_1,\dots,a_{n-1})/\mathfrak{M}) = t((b_0,b_1,\dots,b_{n-1})/\mathfrak{N})$. *Alors, pour tout* $a \in M$, *il existe* $b \in N$ *tel que* $t((a_0,a_1,\dots,a_{n-1},a)/\mathfrak{M}) = t((b_0,b_1,\dots,b_{n-1},b)/\mathfrak{N})$.

☹ Posons $p = t((a_0,a_1,\dots,a_{n-1})/\mathfrak{M})$ et $q = t((a_0,a_1,\dots,a_{n-1},a)/\mathfrak{M})$; soient $F_1[v_0,v_1,\dots,v_{n-1}]$ et $F_2[v_0,v_1,\dots,v_{n-1},v_n]$ des formules isolant respectivement p et q. On voit alors que $\exists v_n F_2[v_0,v_1,\dots,v_{n-1},v_n] \in p$, et, puisque $t((b_0,b_1,\dots,b_{n-1})/\mathfrak{N}) = p$,

$$\mathfrak{N} \models \exists v_n F_2[b_0,b_1,\dots,b_{n-1},v_n].$$

Soit donc b un point de N tel que $\mathfrak{N} \models F_2[b_0,b_1,\dots,b_{n-1},b]$. Alors $t((b_0,b_1,\dots,b_{n-1},b)/\mathfrak{N}) = q$.
☺

LEMME 2 : *On reprend les hypothèses du lemme 1. Soient* $\mathfrak{M}$ *et* $\mathfrak{N}$ *deux modèles dénombrables de* T, $(a_0,a_1,\dots,a_{n-1})$ et $(b_0,b_1,\dots,b_{n-1})$ *des suites de* M *et* N *respectivement telles que* $t((a_0,a_1,\dots,a_{n-1})/\mathfrak{M}) = t((b_0,b_1,\dots,b_{n-1})/\mathfrak{N})$. *Alors il existe un isomorphisme* f *de* $\mathfrak{M}$ *sur* $\mathfrak{N}$ *tel que, pour tout* i *compris entre* 0 *et* $n-1$, $f(a_i) = b_i$.

☹ On va construire f par la méthode du va et vient (celle qui nous a servi en 2.7) : soient $(c_i\ ;\ i \in \mathbb{N})$ une énumération de M et $(d_i\ ;\ i \in \mathbb{N})$ une énumération de N. L'application f est déjà déterminée sur l'ensemble $\{a_0,a_1,\dots,a_{n-1}\}$. On va la compléter en définissant par récurrence sur l'entier k, un point a_{n+k} de M et un point b_{n+k} de N, de telle sorte, que pour tout entier k,

(*) $$t((a_0,a_1,\dots,a_{n+k})/\mathfrak{M}) = t((b_0,b_1,\dots,b_{n+k})/\mathfrak{N}).$$

Pour définir a_{n+k} et b_{n+k} en supposant que les points a_i et b_i pour $i < n+k$ aient déjà été définis conformément à (*), on distinguera deux cas :

- Si $k = 2i$ est pair, alors on pose $a_{n+k} = c_i$; par hypothèse de récurrence, on a :

$$t((a_0,a_1,\dots,a_{n+k-1})/\mathfrak{M}) = t((b_0,b_1,\dots,b_{n+k-1})/\mathfrak{N}),$$

et le lemme 1 nous permet de trouver un point b_{n+k} tel que :

$$t((a_0,a_1,\dots,a_{n+k})/\mathfrak{M}) = t((b_0,b_1,\dots,b_{n+k})/\mathfrak{N}).$$

• Si $k = 2i + 1$ est impair, alors on pose $b_{n+k} = d_i$, et on utilise encore le lemme 1 pour trouver un point a_{n+k} tel que $t((a_0,a_1,\dots,a_{n+k})/\mathfrak{M}) = t((b_0,b_1,\dots,b_{n+k})/\mathfrak{N}))$.

On remarque que, quelques soient les entiers m et p, $a_m = a_p$ si et seulement si $b_m = b_p$: en effet, en supposant par exemple que $p \geqslant m$, $a_m = a_p$ si et seulement si $v_m \simeq v_p \in t((a_0,a_1,\dots,a_p)/\mathfrak{M})$, si et seulement si $v_m \simeq v_p \in t((b_0,b_1,\dots,b_p)/\mathfrak{N})$, si et seulement si $b_m = b_p$. On peut donc définir une bijection de l'ensemble $\{a_m ; m \in \mathbb{N}\}$ sur l'ensemble $\{b_m ; m \in \mathbb{N}\}$ en posant : pour tout entier m, $f(a_m) = b_m$. Or le choix de a_{n+k} pour k pair nous assure que $\{a_m ; m \in \mathbb{N}\} = M$, et le choix de b_{n+k} pour k impair que $\{b_m ; m \in \mathbb{N}\} = N$: f est donc une bijection de M sur N.

Cette bijection est un isomorphisme de $\mathfrak{M}$ sur $\mathfrak{N}$: cela découle immédiatement du fait que, pour toute formule $F[v_0,v_1,\dots,v_{m-1}]$, les conditions suivantes sont équivalentes : 1) $\mathfrak{M} \models F[a_0,a_1,\dots,a_{m-1}]$; 2) $F[v_0,v_1,\dots,v_{m-1}] \in t((a_0,a_1,\dots a_{m-1})/\mathfrak{M})$; 3) $F[v_0,v_1,\dots,v_{m-1}] \in t((b_0,b_1,\dots,b_{m-1})/\mathfrak{N})$; 4) $\mathfrak{N} \models F[b_0,b_1,\dots,b_{m-1}]$.

☺

Soient $\mathfrak{M}$ et $\mathfrak{N}$ deux modèles dénombrables de T ; le type complet que la suite vide réalise dans $\mathfrak{M}$ est la théorie de $\mathfrak{M}$, et il est égal au type complet que réalise la suite vide dans $\mathfrak{N}$ (parce que, T étant complète, on a $Th(\mathfrak{M}) = Th(\mathfrak{N})$. On peut appliquer le lemme 2, et on voit que $\mathfrak{M}$ et $\mathfrak{N}$ sont isomorphes.

☺

Le lemme 2 a une autre conséquence très intéressante. En considérant le cas où les modèles $\mathfrak{M}$ et $\mathfrak{N}$ sont égaux, on obtient :

PROPOSITION : *Soit* $\mathfrak{M}$ *un modèle dénombrable d'une théorie* $\aleph_0$-*catégorique, et supposons que* $(a_0,a_1,\dots,a_{n-1})$ et $(b_0,b_1,\dots,b_{n-1})$ *soient des suites de* M *telles que* $t((a_0,a_1,\dots,a_{n-1})/\mathfrak{M}) = t((b_0,b_1,\dots,b_{n-1})/\mathfrak{M})$. *Alors il existe un automorphisme* f *de* $\mathfrak{M}$ *tel que, pour tout* i *compris entre* 0 *et* $n-1$, $f(a_i) = b_i$.

6.7 Soit n un entier. On peut définir, sur l'ensemble des formules le L dont les seules variables libres sont v_0, v_1, ..., v_{n-1} une relation $\equiv$ qui manifestement est une relation d'équivalence par : pour toutes formules $F[v_0,v_1,\dots,v_{n-1}]$ et $G[v_0,v_1,\dots,v_{n-1}]$, $F[v_0,v_1,\dots,v_{n-1}] \equiv G[v_0,v_1,\dots,v_{n-1}]$ si et seulement si

$$T \vdash \forall v_0 \forall v_1 \dots \forall v_{n-1}(F[v_0,v_1,\dots,v_{n-1}] \Longleftrightarrow G[v_0,v_1,\dots,v_{n-1}]).$$

Autrement dit, $F[v_0,v_1,\ldots,v_{n-1}] \equiv G[v_0,v_1,\ldots,v_{n-1}]$ si et seulement si pour tout modèle $\mathfrak{M}$ de T et pour toute suite $(a_0,a_1,\ldots,a_{n-1})$ de M,

$$\mathfrak{M} \models F[a_0,a_1,\ldots,a_{n-1}] \Longleftrightarrow G[a_0,a_1,\ldots,a_{n-1}].$$

L'ensemble des classes relativement à cette relation est notée Lind_n (pour : « **algèbre de Lindenbaum** » : c'est naturellement une algèbre de Boole).

Si $F = F[v_0,v_1,\ldots,v_{n-1}]$ est une formule de L, notons :

$$S_n(F) = \{ p \in S_n \ ; \ F \in p \}.$$

Il est d'abord clair que, si deux formules $F = F[v_0,v_1,\ldots,v_{n-1}]$ et $G = G[v_0,v_1,\ldots,v_{n-1}]$ sont équivalentes modulo $\equiv$, alors $S_n(F) = S_n(G)$. Réciproquement, si F et G ne sont pas équivalentes modulo $\equiv$, alors il existe un modèle $\mathfrak{M}$ de T et une suite $(a_0,a_1,\ldots,a_{n-1})$ de points de M vérifiant l'une des formules, disons F, et pas l'autre. Alors $t((a_0,a_1,\ldots,a_{n-1})/\mathfrak{M})$ est dans $S_n(F)$ et pas dans $S_n(G)$: il n'y a donc pas plus d'éléments dans Lind_n que de sous-ensembles de S_n, et, si S_n est un ensemble fini, il en est de même de Lind_n.

Le théorème suivant résume et complète les résultats que nous avons obtenus sur les théories $\aleph_0$-catégoriques :

THEOREME : *Les cinq propriétés suivantes sont équivalentes :*

i) T *est* $\aleph_0$*-catégorique ;*

ii) pour tout entier n, *tout* n*-type consistant est isolé ;*

iii) pour tout entier n, *tout* n*-type complet est isolé ;*

iv) pour tout entier n, *l'ensemble* S_n *est fini ;*

v) pour tout entier n, *l'ensemble* Lind_n *est fini.*

⊖ L'implication *i)* ⟹ *ii)* est le corollaire 1 de 6.5 ; *ii)* ⟹ *iii)* est évident ; *iii)* ⟹ *i)* est le théorème 6.6. Par ailleurs, l'implication *i)* ⟹ *iv)* est le corollaire 2 de 6.5, et on vient de montrer l'implication *iv)* ⟹ *v)*. On terminera en montrant que ¬*iii)* ⟹ ¬*v)*.

On sait par hypothèse qu'il existe un entier n et un n-type p complet et non isolé. On construit par récurrence sur k une suite $(F_k[v_0,v_1,\ldots,v_{n-1}] \ ; \ k \in \mathbb{N})$ de formules appartenant à p, de telle sorte que, pour tout k :

$$T \vdash \forall v_0 \forall v_1 \ldots \forall v_{n-1}(F_{k+1}[v_0,v_1,\ldots,v_{n-1}] \Rightarrow F_k[v_0,v_1,\ldots,v_{n-1}])$$

et $$T \vdash \neg\forall v_0 \forall v_1 \ldots \forall v_{n-1}(F_k[v_0,v_1,\ldots,v_{n-1}] \Rightarrow F_{k+1}[v_0,v_1,\ldots,v_{n-1}]).$$

On part de n'importe quelle formule $F_0[v_0,v_1,\ldots,v_{n-1}]$ de p. Supposons que l'on ait déjà défini $F_k[v_0,v_1,\ldots,v_{n-1}]$. Parce que p n'est pas isolé, on sait qu'il existe une formule $G[v_0,v_1,\ldots,v_{n-1}] \in p$ telle que :

$$T \vdash \neg\forall v_0 \forall v_1 \ldots \forall v_{n-1}(F_k[v_0,v_1,\ldots,v_{n-1}] \Rightarrow G[v_0,v_1,\ldots,v_{n-1}]).$$

On pose $F_{k+1}[v_0,v_1,\ldots,v_{n-1}]) = F_k[v_0,v_1,\ldots,v_{n-1}] \wedge G[v_0,v_1,\ldots,v_{n-1}]$.

Il est alors clair que les formules $F_k[v_0,v_1,\ldots,v_{n-1}]$ pour $k \in \mathbb{N}$ sont deux à deux non équivalentes modulo $\equiv$.

☺

6.8 On dira qu'une **structure est $\aleph_0$-catégorique** si sa théorie complète l'est. Soit $\mathfrak{M}$ une structure dénombrable $\aleph_0$-catégorique. Considérons, pour chaque entier n, la relation binaire R_n sur M^n définie par : pour toutes suites $(a_0,a_1,\ldots,a_{n-1})$ et $(b_0,b_1,\ldots,b_{n-1})$, $R_n((a_0,a_1,\ldots,a_{n-1}),(b_0,b_1,\ldots,b_{n-1}))$ si et seulement si il existe un automorphisme f de $\mathfrak{M}$ tel que, pour tout i compris 0 et $n-1$, $f(a_i) = b_i$. Il est facile de voir que cette relation est une relation d'équivalence. On peut remarquer que l'ensemble des automorphismes de $\mathfrak{M}$ est un sous-groupe du groupe des permutations de M, et on voit que les classes modulo R_n ne sont rien d'autres que les orbites pour l'action de ce groupe G sur M^n.

On a vu (proposition 6.6), que si deux suites de M de même longueur réalisent le même type complet, alors il existe un automorphisme de $\mathfrak{M}$ envoyant la première dans la seconde, autrement dit, qu'elles sont équivalentes modulo R_n. La réciproque est évidente. Ceci, avec le théorème 6.7, nous permet de donner une caractérisation purement algébrique (aucune référence à la notion de formule) des structures $\aleph_0$-catégoriques :

THEOREME : *Soit $\mathfrak{M}$ une structure dénombrable. Alors les conditions suivantes sont équivalentes :*

i) $\mathfrak{M}$ est $\aleph_0$-catégorique ;

ii) pour tout entier n, la relation R_n définie ci-dessus n'a qu'un nombre fini de classes.

EXERCICES

1. On considère un langage du premier ordre L comportant deux symboles de prédicat unaire E et P et un symbole de prédicat binaire A. On appelle T la théorie de L constituée des formules suivantes :

H_0 : $\forall v_0(Ev_0 \Longleftrightarrow \neg Pv_0)$

H_1 : $\forall v_0 \forall v_1(Av_0v_1 \Longrightarrow (Ev_0 \wedge Pv_1))$

H_2 : $\forall v_1 \forall v_2((Pv_1 \wedge Pv_2 \wedge \forall v_0(Av_0v_1 \Longleftrightarrow Av_0v_2)) \Longrightarrow v_1 \simeq v_2)$

H_3 : $\exists v_0(Pv_0 \wedge \forall v_1 \neg Av_1v_0)$

H_4 : $\forall v_1(Pv_1 \Longrightarrow \exists v_2(Pv_2 \wedge \forall v_0(Ev_0 \Longrightarrow (Av_0v_1 \Longleftrightarrow \neg Av_0v_2))))$

H_5 : $\forall v_1 \forall v_2 \exists v_3((Pv_1 \wedge Pv_2) \Longrightarrow \forall v_0(Av_0v_3 \Longleftrightarrow (Av_0v_1 \vee Av_0v_2)))$

et, pour chaque entier $n \geqslant 1$, de la formule F_n :

$$\forall v_1 \forall v_2 \ldots \forall v_n((\bigwedge_{1 \leqslant i \leqslant n} Ev_i) \Longrightarrow \exists w_1 \forall w_0(Aw_0w_1 \Longleftrightarrow (\bigvee_{1 \leqslant i \leqslant n} w_0 \simeq v_i))).$$

a) Soient X un ensemble non vide et $\mathscr{P}(X)$ l'ensemble de ses parties, que l'on suppose disjoint de X. On définit une L-structure $\mathfrak{M}_X$ de la manière suivante :

- l'ensemble de base est $M_X = X \cup \mathscr{P}(X)$;
- l'interprétation de E est X ;
- l'interprétation de P est $\mathscr{P}(X)$;
- l'interprétation de A est l'ensemble $\overline{A} = \{(x,y) \in M_X^2 ; x \in X, y \in \mathscr{P}(X) \text{ et } x \in y\}$.

Montrer que M_X est un modèle de T.

b) Existe-t-il un modèle dénombrable de T ?

c) Quels sont les entiers n pour lesquels T admet un modèle dont l'ensemble de base admet n éléments ?

d) Démontrer que T est équivalente à $\{H_0, H_1, H_3, H_4, H_5, F_1\}$.

e) Montrer que T n'est pas $\aleph_0$-catégorique.

2. On reprend l'exercice 15 du chapitre 3.

a) Soit $\mathfrak{M} = \langle M, \overline{d}, \overline{g} \rangle$ un modèle quelconque de T.

On définit sur M une relation binaire $\approx$ par :

$a \approx b$ si et seulement si il existe des entiers naturels m, n, p et q tels que :

$$\overline{d}^m(\overline{g}^n(a)) = \overline{d}^p(\overline{g}^q(b)).$$

Montrer que $\approx$ est une relation d'équivalence sur M. Chaque classe d'équivalence pour $\approx$ sera appelée une **grille**.

Montrer que chaque grille est stable pour $\overline{d}$ et $\overline{g}$.

Montrer que chaque grille, munie des restrictions des applications $\overline{d}$ et $\overline{g}$, est une sous-structure de $\mathfrak{M}$ qui est un modèle de T.

b) Soit L' le langage obtenu en ajoutant à L deux nouveaux symboles : des symboles de constante λ et μ. Pour chaque quadruplet (m,n,p,q) d'entiers naturels, on appelle G_{mnpq} la formule close de L' :

$$\neg d^m g^n \lambda \simeq d^p g^q \mu.$$

En utilisant cette famille de formules, démontrer l'existence d'un modèle non standard de T (c'est-à-dire d'un modèle de T non isomorphe au modèle standard).

c) Soit A un ensemble non vide. Construire un modèle de T dont l'ensemble de grilles est équipotent à A.

d) Montrer que deux modèles de T ayant des ensembles de grilles équipotents sont isomorphes.

e) Montrer que T n'est pas $\aleph_0$-catégorique. On considère un ensemble $\mathscr{X}$ de L-structures ayant les propriétés suivantes :

- les éléments de $\mathscr{X}$ sont des modèles dénombrables de T ;
- si $\mathfrak{M} \in \mathscr{X}$, $\mathfrak{N} \in \mathscr{X}$ et $\mathfrak{M} \neq \mathfrak{N}$, alors $\mathfrak{M}$ et $\mathfrak{N}$ ne sont pas isomorphes ;
- tout modèle dénombrable de T est isomorphe à un des éléments de $\mathscr{X}$.

Quel est le cardinal de $\mathscr{X}$?

f) Soit κ un cardinal infini non dénombrable. Montrer que T est κ-catégorique.

3. Soit $<G,.,e>$ un groupe. On lui associe un langage du premier ordre L_G comportant, pour chaque élément $\alpha \in G$, un symbole de fonction unaire f_α.

On désigne par T la théorie suivante de L_G :

$$\{\forall v_0 f_e v_0 \simeq v_0\} \cup \{\forall v_0 f_\alpha f_\beta v_0 \simeq f_{\alpha\beta} v_0 \ ; \ \alpha \in G, \beta \in G\} \cup \{\forall v_0 \neg f_\alpha v_0 \simeq v_0 \ ; \ \alpha \in G, \alpha \neq e\}.$$

a) Montrer que, pour tout terme t de L_G, il existe un élément $\alpha \in G$, et un symbole de variable x, tels que :

$$T \vdash \forall x\, t \simeq f_\alpha x.$$

b) Après avoir remarqué que chaque formule atomique de L_G comporte au plus deux variables, montrer que, pour toute formule atomique $F = F[v_0,v_1]$ de L_G, on a une des trois possibilités suivantes :

- $T \vdash \forall v_0 \forall v_1 F$;
- $T \vdash \forall v_0 \forall v_1 \neg F$;
- il existe un élément $\alpha \in G$ tel que : $T \vdash \forall v_0 \forall v_1 (F \Longleftrightarrow v_0 \simeq f_\alpha v_1)$.

c) Montrer que la L_G-structure $\mathfrak{G}$, dont l'ensemble de base est G et où, pour chaque $\alpha \in G$, le symbole f_α est interprété par l'application $\beta \mapsto \alpha.\beta$ de G dans G (multiplication à gauche par α), est un modèle de T.

d) Soit $\mathfrak{M} = < M, (\varphi_\alpha)_{\alpha\in G} >$ un modèle de T et soit a un élément de M. On considère l'ensemble :

$$O(a) = \{ x \in M \text{ ; il existe } \alpha \in G \text{ tel que } x = \varphi_\alpha(a) \}.$$

Montrer que O(a) est une sous-structure de $\mathfrak{M}$ qui est isomorphe à $\mathfrak{G}$. Montrer que :

$$X_M = \{ O(a) \text{ ; } a \in M \}$$

est une partition de M. Montrer que si $\mathfrak{M}$ et $\mathfrak{N}$ sont deux modèles de T et si X_M et X_N sont équipotents, alors $\mathfrak{M}$ et $\mathfrak{N}$ sont isomorphes.

e) Montrer que, si G est infini, la théorie T est complète.

f) On suppose que G est fini. Existe-t-il un cardinal infini λ tel que T soit λ-catégorique ? La théorie T est-elle complète ?

4. On considère le langage L constitué d'un symbole de relation binaire R. On appelle L_∞ le langage obtenu en ajoutant à L une infinité dénombrable de nouveaux symboles de constante : $c_0, c_1, c_2, \ldots, c_n, \ldots$

Pour chaque entier n, on appelle L_n le langage $L \cup \{c_0, c_1, c_2, \ldots, c_n\}$.

Etant donnés une L_∞-structure $\mathfrak{M}$ et un entier n, on notera $\mathfrak{M}_n$ la L_n-structure qui est le réduit de $\mathfrak{M}$ au langage L_n.

On considère une théorie T du langage L qui exprime que l'interprétation de R est une relation d'équivalence admettant une infinité de classes d'équivalences qui sont toutes infinies.

a) Ecrire des axiomes pour la théorie T et donner un exemple de modèle de T.

b) Montrer que T n'est équivalente à aucune théorie finie de L.

c) Pour quels cardinaux infinis λ la théorie T est-elle λ-catégorique ? Trouver deux modèles $\mathfrak{M}_1$ et $\mathfrak{M}_2$ de T tels qu'il n'existe ni injection élémentaire de $\mathfrak{M}_1$ dans $\mathfrak{M}_2$, ni injection élémentaire de $\mathfrak{M}_2$ dans $\mathfrak{M}_1$.

d) La théorie T est-elle complète ?

e) Soit T_+ la théorie suivante du langage L_∞ :

$$T_+ = T \cup \{ \neg R c_n c_m \text{ ; } n \in \mathbb{N}, m \in \mathbb{N} \text{ et } n \neq m \}.$$

Donner un exemple de modèle de T_+.

Montrer que T_+ n'est équivalente à aucune théorie finie du langage L_∞.

f) Pour quels cardinaux infinis λ la théorie T_+ est-elle λ-catégorique ?

g) Soient $\mathfrak{M}_1$ et $\mathfrak{M}_2$ deux modèles dénombrables de T_+. Montrer que, pour tout $n \in \mathbb{N}$, les réduits de $\mathfrak{M}_1$ et $\mathfrak{M}_2$ au langage L, que l'on désignera respectivement par $\mathfrak{M}_1\restriction_{L_n}$ et $\mathfrak{M}_2\restriction_{L_n}$, sont isomorphes. En conclure que T_+ est une théorie complète de L_∞.

5. On considère un langage du premier ordre L dénombrable et on désigne par $\mathcal{F}_1$ l'ensemble des formules à une variable libre (au plus) de L.

Etant données une formule $F[x] \in \mathcal{F}_1$ et une L-structure $\mathfrak{M} = \langle M, \ldots \rangle$, on appelle **valeur de F dans $\mathfrak{M}$**, et on note $Val(F,\mathfrak{M})$, le sous-ensemble de M que définit la formule F, c'est-à-dire l'ensemble :

$$Val(F,\mathfrak{M}) = \{ a \in M \ ; \ \mathfrak{M} \models F[a] \}.$$

Pour chaque cardinal infini λ, on appelle **λ-structure** toute L-structure infinie $\mathfrak{M}$ vérifiant la propriété suivante :

La valeur de chaque formule $F \in \mathcal{F}_1$ dans $\mathfrak{M}$ est : soit un ensemble fini, soit un ensemble de cardinal λ.

On appellera **λ-modèle** d'une formule ou d'une théorie tout modèle de cette formule ou de cette théorie qui est une λ-structure.

a) Montrer que, si λ est un cardinal infini, toute λ-structure est de cardinal λ.

b) Montrer que toute structure de cardinal $\aleph_0$ est une $\aleph_0$-structure.

c) Soient T une théorie de L et F[x] une formule de $\mathcal{F}_1$. On suppose que, pour tout entier n, T admet un modèle dans lequel la valeur de la formule F est un ensemble à au moins n éléments.

Montrer que, pour tout cardinal infini λ, T admet au moins un modèle dans lequel la valeur de F est un ensemble de cardinal égal à λ.
(Indication : ajouter au langage un ensemble de symboles de constante de cardinal λ).

d) Soit T une théorie de L qui admet au moins un modèle infini. Montrer que, pour tout cardinal infini λ, T admet au moins un λ-modèle.
(Indication : choisir un modèle infini $\mathfrak{M}_0$ de T, et, à chaque formule $G \in \mathcal{F}_1$ dont la valeur dans $\mathfrak{M}_0$ est un ensemble infini, associer un ensemble de symboles de constante C_G de cardinal λ).

e) Soit S une théorie non contradictoire de L qui n'admet que des modèles infinis. On suppose qu'il existe au moins un cardinal infini λ tel que tous les λ-modèles de S soient isomorphes. Montrer que S est complète.

6. On considère les langages $L_1 = \{ f \}$ et $L_2 = \{ f, P \}$ où f est un symbole de fonction unaire et P un symbole de relation unaire. On appelle T_1 la théorie de L_1 suivante :

$$\{ \forall x \forall y (fx \simeq fy \Longrightarrow x \simeq y) \ , \ \forall x \exists y fy \simeq x \} \cup \{ \forall x \neg f^n x \simeq x \ ; \ n \in \mathbb{N}^* \}.$$

(Le terme $f^n x$ étant défini comme d'habitude : $f^0 x = x$ et, pour tout $n \in \mathbb{N}$, $f^{n+1}x = ff^n x$).

On appelle T_2 la théorie de L_2 suivante :

$$T_1 \cup \{ \exists x Px \ , \ \exists x \neg Px \ , \ \forall x (Px \Longleftrightarrow Pfx) \}.$$

a) Montrer que T_1 est une théorie complète de L_1.

b) Montrer que T_2 n'est catégorique en aucun cardinal infini.

c) En utilisant les résultats de l'exercice précédent, montrer que T_2 est une théorie complète de L_2.

7. a) Soit L_0 le langage comportant un unique symbole de prédicat binaire R. On appelle T_0 la théorie contenant, d'une part les axiomes exprimant que R s'interprète comme un ordre total, d'autre part les deux formules suivantes :

$$\forall v_1 \exists v_2 (Rv_1v_2 \wedge \neg v_1 \simeq v_2 \wedge \forall v_3((Rv_1v_3 \wedge \neg v_1 \simeq v_3) \Longrightarrow Rv_2v_3))\ ;$$
$$\forall v_1 \exists v_2 (Rv_2v_1 \wedge \neg v_1 \simeq v_2 \wedge \forall v_3((Rv_3v_1 \wedge \neg v_1 \simeq v_3) \Longrightarrow Rv_3v_2)).$$

Montrer qu'on peut trouver deux modèles $\mathfrak{M}_0$ et $\mathfrak{M}_1$ de T_0 tels que $\mathfrak{M}_0$ soit une sous-structure de $\mathfrak{M}_1$ sans en être une sous-structure élémentaire.

b) Montrer que T_0 n'est équivalente à aucune théorie $\forall\exists$ de L_0 (voir 5.5).

8. Soient L un langage dénombrable et T une théorie non contradictoire de L qui n'admet que des modèles infinis.

On dit que T est **modèle-complète** si et seulement si, quels que soient les modèles $\mathfrak{M}$ et $\mathfrak{N}$ de T, si $\mathfrak{N}$ est une extension de $\mathfrak{M}$, c'en est une extension élémentaire.

On dit qu'un modèle $\mathfrak{M}$ de T est un **modèle premier de** T si et seulement si tout modèle de T est isomorphe à une extension (simple) de $\mathfrak{M}$.

a) Montrer que toute théorie modèle-complète qui admet un modèle premier est complète.

b) Montrer que les quatre conditions suivantes sont équivalentes :

1°) T est modèle-complète ;

2°) pour tout modèle $\mathfrak{M}$ de T, toute formule de $D(\mathfrak{M})$ est conséquence de $\Delta(\mathfrak{M}) \cup T$ (voir 2.3 pour les notations) ;

3°) pour tout modèle dénombrable $\mathfrak{M}$ de T, toute formule de $D(\mathfrak{M})$ est conséquence de $\Delta(\mathfrak{M}) \cup T$;

4°) pour tous modèles dénombrables $\mathfrak{M}$ et $\mathfrak{M}'$ de T, si $\mathfrak{M} \subseteq \mathfrak{M}'$, alors $\mathfrak{M} \prec \mathfrak{M}'$.

c) Montrer que, si T est modèle-complète, T est équivalente à une théorie $\forall\exists$. La réciproque est-elle vraie ?.

d) Soit $F[v_0,v_1,\dots,v_n]$ une formule de L. On considère la condition suivante portant sur T et $F[v_0,v_1,\dots,v_n]$:

(*) pour tous modèles $\mathfrak{M}$ et $\mathfrak{M}'$ de T tels que $\mathfrak{M} \subseteq \mathfrak{M}'$, pour tous éléments a_0, $a_1, \dots, a_n$ de M, si $\mathfrak{M} \models F[a_0,a_1,\dots,a_n]$ alors $\mathfrak{M}' \models F[a_0,a_1,\dots,a_n]$

Montrer que $F[v_0,v_1,\dots,v_n]$ satisfait (*) si et seulement si il existe une formule existentielle $G[v_0,v_1,\dots,v_n]$ de L telle que :

$$T \vdash \forall v_0 \forall v_1 \dots \forall v_n (F[v_0,v_1,\dots,v_n] \Longleftrightarrow G[v_0,v_1,\dots,v_n]).$$

(Indication : ajouter des symboles de constante $c_0, c_1, \dots, c_n$ et s'inspirer de la preuve du théorème 5.2.)

e) Montrer que T est modèle-complète si et seulement si, pour toute formule universelle $F[v_0,v_1,\ldots,v_n]$ de L, il existe une formule existentielle $G[v_0,v_1,\ldots,v_n]$ de L telle que :

$$T \vdash \forall v_0 \forall v_1 \ldots \forall v_n (F[v_0,v_1,\ldots,v_n] \Longleftrightarrow G[v_0,v_1,\ldots,v_n]).$$

9. Le but de cet exercice est la démonstration du **théorème de Lindström** : *soit* T *une théorie* $\forall\exists$ *dans un langage dénombrable ; si* T *n'admet pas de modèle fini et est catégorique en un cardinal infini, alors* T *est modèle-complète.*

On reprend les notations et les résultats de l'exercice 8.

a) Soient λ un cardinal infini et $F[v_0,v_1,\ldots,v_n]$ une formule de L. Montrer que les deux conditions suivantes sont équivalentes :

1°) pour tous modèles $\mathfrak{M}$ et $\mathfrak{M}'$ de T de cardinalité λ tels que $\mathfrak{M} \subseteq \mathfrak{M}'$, pour tous éléments $a_0, a_1, \ldots, a_n$ de M, si $\mathfrak{M} \models F[a_0,a_1,\ldots,a_n]$ alors $\mathfrak{M}' \models F[a_0,a_1,\ldots,a_n]$.

2°) il existe une formule existentielle $G[v_0,v_1,\ldots,v_n]$ de L telle que :

$$T \vdash \forall v_0 \forall v_1 \ldots \forall v_n (F[v_0,v_1,\ldots,v_n] \Longleftrightarrow G[v_0,v_1,\ldots,v_n]).$$

b) On suppose que T est une théorie $\forall\exists$. Soient $F[v_0,v_1,\ldots,v_n]$ une formule universelle et λ un cardinal infini. Montrer que T admet un modèle $\mathfrak{M}$ de cardinalité λ possédant la propriété suivante :

(•) pour tout modèle $\mathfrak{M}'$ de T tel que $\mathfrak{M} \subseteq \mathfrak{M}'$, pour tous éléments $a_0, a_1, \ldots, a_n$ de M, si $\mathfrak{M} \models F[a_0,a_1,\ldots,a_n]$, alors $\mathfrak{M}' \models F[a_0,a_1,\ldots,a_n]$.

c) Démontrer le théorème de Lindström.

d) Le langage étant constitué d'un symbole de fonction unaire f, on pose :

$$T_0 = \{\forall v_0 \forall v_1 (fv_0 \simeq fv_1 \Rightarrow v_0 \simeq v_1)\} \cup \{\forall v_0 \neg f^n v_0 \simeq v_0 \,;\, n \in \mathbb{N}\} .$$

Montrer que T_0 est une théorie $\forall\exists$ qui n'est ni complète ni modèle-complète.

En enrichissant le langage et en ajoutant des axiomes à T_0, construire une théorie $\forall\exists$, complète, qui ne soit pas modèle complète.

10. Le langage L est constitué d'un symbole de prédicat binaire R et d'un ensemble infini dénombrable de symboles de constantes : $\{c_0,c_1,\ldots,c_n,\ldots\}$.

Soit A une formule close de L exprimant que R s'interprète comme un ordre strict total dense sans extrémités. Pour chaque $n \in \mathbb{N}$, F_n est la formule Rc_nc_{n+1}.

On considère la théorie :

$$T = \{A\} \cup \{F_n \,;\, n \in \mathbb{N}\}.$$

On désigne par $\mathfrak{A}$, $\mathfrak{B}$ et $\mathfrak{C}$ les trois L-structures dont l'ensemble de base est $\mathbb{Q}$, où R s'interprète comme l'ordre strict usuel, et où la suite de symboles de constante $(c_n)_{n\in\mathbb{N}}$ est interprétée respectivement par les suites de rationnels :

$$\alpha = (\alpha_n)_{n\in\mathbb{N}},\ \beta = (\beta_n)_{n\in\mathbb{N}} \text{ et } \gamma = (\gamma_n)_{n\in\mathbb{N}},$$

ainsi définies : pour tout $n \in \mathbb{N}$,

$$\alpha_n = n \quad ; \quad \beta_n = -\frac{1}{n+1} \quad ; \quad \gamma_n = \sum_{k=0}^{n} \frac{1}{k!}\ .$$

a) Montrer que T est complète dans L.

b) Montrer que tout modèle dénombrable de T est isomorphe à l'une des trois L-structures $\mathfrak{A}$, $\mathfrak{B}$ et $\mathfrak{C}$.

c) Montrer que la théorie T est modèle-complète (voir l'exercice 8).

d) Montrer que tout modèle dénombrable de T admet une extension élémentaire isomorphe à $\mathfrak{B}$ et une extension élémentaire isomorphe à $\mathfrak{C}$.

11. Soit L le langage du premier ordre constitué d'un symbole de fonction unaire f et d'un symbole de prédicat binaire R. On appelle A la conjonction des formules suivantes :

$\forall v_0 Rv_0v_0$;
$\forall v_0 \forall v_1 ((Rv_0v_1 \Longleftrightarrow Rv_1v_0) \Longrightarrow v_0 \simeq v_1)$;
$\forall v_0 \forall v_1 \forall v_2 ((Rv_0v_1 \wedge Rv_1v_2) \Longrightarrow Rv_0v_2)$;
$\forall v_0 \forall v_1 (Rv_0v_1 \Longleftrightarrow Rfv_0fv_1)$;
$\forall v_0 (Rv_0fv_0 \wedge \neg v_0 \simeq fv_0)$;
$\forall v_0 \forall v_1 ((\neg v_0 \simeq v_1 \wedge Rv_0v_1) \Longrightarrow Rfv_0v_1)$.

a) Montrer que, dans tout modèle de la formule A, l'interprétation du symbole R est une relation d'ordre total sur l'ensemble de base du modèle, sans plus petit ni plus grand élément, telle que tout élément admette un successeur, c'est-à-dire un plus petit majorant strict.

b) Montrer que $\mathbb{Z}$ muni de la relation d'ordre habituelle et de la fonction successeur est un modèle de A.

Soit $X = \langle B, \leqslant \rangle$ un ensemble totalement ordonné quelconque. On considère la L-structure $\mathfrak{M}_X$ suivante :

– l'ensemble de base de $\mathfrak{M}_X$ est l'ensemble $B \times \mathbb{Z}$;

– l'interprétation de R dans $\mathfrak{M}_X$ est l'ensemble

$$\{ ((x,n),(y,m) \in (B \times \mathbb{Z})^2 \ ; \ x < y \text{ ou } (x = y \text{ et } n \leqslant m) \} \ ;$$

– l'interprétation de f dans $\mathfrak{M}_X$ est l'application qui à $(x,n) \in (B \times \mathbb{Z})$ fait correspondre $(x, n+1)$.

Montrer que $\mathfrak{M}_X$ est un modèle de A.

c) Soit $\mathfrak{M} = \langle M, \bar{f}, \bar{R} \rangle$ un modèle de A. On veut montrer qu'il existe un ensemble totalement ordonné X tel que $\mathfrak{M}$ soit isomorphe à $\mathfrak{M}_X$.

On définit la relation $\ll$ binaire sur $\mathfrak{M}$ par : pour tous a, b dans $\mathfrak{M}$, $a \ll b$ si et

seulement si, pour tout $n \in \mathbb{N}$, $\mathfrak{M} \models Rf^n a\, b$.

Montrer que cette relation est transitive et antiréflexive. Montrer que la relation

$a \approx b$ si et seulement si il existe des entiers n et p tels que $\mathfrak{M} \models f^n a \simeq f^p b$

est une relation d'équivalence et que

$a \approx b$ si et seulement si $a \ll b$ et $b \ll a$ sont tous les deux faux.

Montrer que chaque classe modulo $\approx$ est une sous-structure de $\mathfrak{M}$ isomorphe à $\mathbb{Z}$. Montrer que la relation $\ll$ permet de définir sur l'ensemble $M/\approx$ des classes une relation d'ordre totale.

Montrer que, si $X = \langle C, \triangleleft \rangle$ est l'ensemble ordonné ainsi obtenu, alors $\mathfrak{M}$ est isomorphe à $\mathfrak{M}_X$.

d) Montrer que si X et Y sont deux ensembles totalement ordonnés, alors $\mathfrak{M}_X$ et $\mathfrak{M}_Y$ sont isomorphes si et seulement si X et Y sont isomorphes.

Montrer que A n'a que des modèles infinis et n'est catégorique en aucun cardinal infini.

e) On veut montrer que $\{A\}$ est une théorie complète.

1°) Montrer que, si a et b sont deux points dans un modèle $\mathfrak{M}$ de A et si $a \ll b$, alors il existe une extension élémentaire $\mathfrak{M}_1$ de $\mathfrak{M}$, et un point c dans $\mathfrak{M}_1$, tels que :

$$a \ll c \quad \text{et} \quad c \ll b.$$

2°) Montrer de même que, si a est un point de M, alors il existe une extension élémentaire $\mathfrak{M}_1$ de $\mathfrak{M}$ et des points b et c de M_1 tels que :

$$b \ll a \quad \text{et} \quad a \ll c.$$

3°) Soient $\mathfrak{M}$ et $\mathfrak{N}$ deux modèles de A, $(a_1,a_2,\dots,a_n)$ et $(b_1,b_2,\dots,b_n)$ deux suites finies de même longueur d'éléments de $\mathfrak{M}$ et $\mathfrak{N}$ respectivement. On considère la condition suivante :

$P((\mathfrak{M}, a_1,a_2,\dots,a_n), (\mathfrak{N}, b_1,b_2,\dots,b_n))$: pour toute formule atomique $F[v_1,v_2,\dots,v_n]$ de L,

$\mathfrak{M} \models F[a_1,a_2,\dots,a_n]$ si et seulement si $\mathfrak{N} \models F[b_1,b_2,\dots,b_n]$.

Montrer que la condition $P((\mathfrak{M}, a_1,a_2,\dots,a_n), (\mathfrak{N}, b_1,b_2,\dots,b_n))$ est équivalente à :
Pour tous entiers i et j tels que $1 \leqslant i, j \leqslant n$, pour tout $k \in \mathbb{N}$, ($\mathfrak{M} \models a_i \simeq f^k a_j$ si et seulement si $\mathfrak{N} \models b_i \simeq f^k b_j$) et ($\mathfrak{M} \models Ra_i a_j$ si et seulement si $\mathfrak{N} \models Rb_i b_j$).

4°) On suppose que la condition $P((\mathfrak{M}, a_1,a_2,\dots,a_n), (\mathfrak{N}, b_1,b_2,\dots,b_n))$ est satisfaite. Montrer que, si c est un élément de $\mathfrak{M}$, alors :

– s'il existe un indice i compris entre 1 et n tel que $c \approx a_i$, alors il existe un point d de $\mathfrak{N}$ tel que $P((\mathfrak{M}, a_1,a_2,\dots,a_n,c), (\mathfrak{N}, b_1,b_2,\dots,b_n,d))$;

– sinon, il existe une extension élémentaire $\mathfrak{N}'$ de $\mathfrak{N}$ et un point d de $\mathfrak{N}'$ tels que $P((\mathfrak{M}, a_1,a_2,\dots,a_n,c), (\mathfrak{N}', b_1,b_2,\dots,b_n,d))$.

5°) Montrer l'assertion suivante par induction sur la hauteur de la formule $G[v_1,v_2,\ldots,v_n]$ de L :

si $\mathfrak{M}$ et $\mathfrak{N}$ sont deux modèles de A, si $(a_1,a_2,\ldots,a_n)$ et $(b_1,b_2,\ldots,b_n)$ sont deux suites finies d'éléments de $\mathfrak{M}$ et $\mathfrak{N}$ respectivement, alors $P((\mathfrak{M}, a_1,a_2,\ldots,a_n), (\mathfrak{N}, b_1,b_2,\ldots,b_n))$ implique :

$$\mathfrak{M} \models G[a_1,a_2,\ldots,a_n] \text{ si et seulement si } \mathfrak{N} \models G[b_1,b_2,\ldots,b_n].$$

6°) En conclure que $\{A\}$ est une théorie complète.

12. Soient L le langage ne comportant qu'un symbole de prédicat binaire $\leqslant$ et T la théorie des ordres denses sans premier ni dernier élément (voir 1.3). Montrer que, pour toute formule $F[v_0,v_1,\ldots,v_n]$, il existe une formule sans quantificateur $H[v_0,v_1,\ldots,v_n]$ telle que :

$$T \vdash \forall v_0 \forall v_1 \ldots \forall v_n (F[v_0,v_1,\ldots,v_n] \Longleftrightarrow H[v_0,v_1,\ldots,v_n]).$$

13. Soit L un langage. On dit qu'une classe $\mathscr{C}$ de L-structures est close par ultraproduit si, pour tout ensemble I, pour tout ultrafitre $\mathscr{U}$ sur I, pour toute suite $(\mathfrak{M}_i\ ;\ i \in I)$ de structures appartenant à $\mathscr{C}$, $\prod_{i \in I} \mathfrak{M}_i / \mathscr{U}$ appartient à $\mathscr{C}$.

Soit T une théorie dans L. Montrer que la classe des L-structures qui ne sont pas modèles de T est close par ultraproduit si et seulement si T est finiment axiomatisable.

14. Soit K un corps (le langage est $(0,1,+,\times)$). Soient I un ensemble et $\mathscr{F}$ un filtre sur I.

a) Montrer que $K^I/\mathscr{F}$ est un anneau et que c'est un corps si et seulement si $\mathscr{F}$ est un ultrafiltre.

b) Soit $\mathscr{J}$ le sous-ensemble de K^I défini par :

$$\mathscr{J} = \{(k_i\ ;\ i \in I) \in K^I\ ;\ \{i \in I\ ;\ k_i = 0\} \in \mathscr{F}\}.$$

Montrer que $\mathscr{J}$ est un idéal de l'anneau K^I et que l'anneau quotient $K^I/\mathscr{J}$ est égal à $K^I/\mathscr{F}$.

15. Le langage est celui des ensembles ordonnés : $L = \{\leqslant\}$.

a) Soit α un ordinal infini. Montrer qu'il existe un ensemble ordonné, élémentairement équivalent à $< \alpha, \leqslant >$, qui ne soit pas bien ordonné.

b) Montrer qu'il existe un ordinal dénombrable α tel que :

$$< \alpha, \leqslant > \prec < \aleph_1, \leqslant > .$$

($\aleph_1$ désigne le premier ordinal non dénombrable.)

c) Montrer qu'il existe deux ordinaux dénombrables distints α et β tels que :

$$< \alpha, \leqslant > \prec < \beta, \leqslant >.$$

16. On considère le langage L (non dénombrable) comprenant : pour chaque entier n, un symbole de constante $\underline{n}$; pour chaque sous-ensemble A de $\mathbb{N}$, un symbole de prédicat unaire $\underline{A}$; pour chaque application f de $\mathbb{N}$ dans $\mathbb{N}$, un symbole de fonction unaire $\underline{f}$. Soit $\mathfrak{N}$ la L-structure dont l'ensemble de base est $\mathbb{N}$, et où chaque symbole $\underline{X}$ de L est interprété par X. Soit T la théorie de $\mathfrak{N}$.

a) Montrer que chaque modèle de T est isomorphe à une extension élémentaire de $\mathfrak{N}$.

b) Soient $\mathfrak{M}$ une extension élémentaire propre de $\mathfrak{N}$ et a un point de M n'appartenant pas à $\mathbb{N}$. Montrer que l'ensemble :

$$\mathcal{F}_a = \{ A \subseteq \mathbb{N} ; \mathfrak{M} \models \underline{A}a \}$$

est un ultrafitre non trivial sur $\mathbb{N}$.

c) Soit α une bijection de $\mathbb{N}^2$ dans $\mathbb{N}$. Pour chaque nombre réel positif r, on choisit deux suites de nombres entiers $(p_r(n) ; n \in \mathbb{N})$ et $(q_r(n) ; n \in \mathbb{N})$ telles que la suite $(p_r(n)/q_r(n) ; n \in \mathbb{N})$ soit convergente de limite r. On définit l'application f_r de $\mathbb{N}$ dans $\mathbb{N}$ par : pour tout $n \in \mathbb{N}$, $f_r(n) = \alpha(p_r(n),q_r(n))$.

Montrer que, si r et s sont deux réels positifs distincts, alors l'ensemble :

$$\{ n \in \mathbb{N} ; f_r(n) = f_s(n) \}$$

est fini.

d) Montrer que tout modèle de T non isomorphe à $\mathfrak{N}$ a une cardinalité supérieure ou égale à $2^{\aleph_0}$. Montrer que T est $\aleph_0$-catégorique.

e) Soient L' le langage obtenu en ajoutant à L un nouveau symbole de prédicat unaire X et T' la théorie : $T \cup \{ X\underline{n} ; n \in \mathbb{N} \}$. Montrer que T' n'admet pas de modèle fini, est $\aleph_0$-catégorique et n'est pas complète.

17. a) Montrer que toute théorie du premier ordre équivalente à une théorie existentielle est préservée par extension (voir 5.4).

On considère désormais une théorie T dans un langage L, préservée par extension. On va prouver qu'elle est équivalente à une théorie existentielle. Pour toute formule G, on note U(G) l'ensemble des formules closes de L qui sont conséquences de G.

b) Montrer que, pour toute formule $F \in T$, la théorie $T \cup U(\neg F)$ est contradictoire (utiliser l'exercice 19 du chapitre 3).

c) Montrer que, pour toute formule $F \in T$, on peut choisir une formule G_F dans $U(\neg F)$ telle que $T \vdash \neg G_F$.

d) En déduire que T est équivalente à la théorie $\{\neg G_F ; F \in T\}$, donc à une théorie existentielle.

Solutions des exercices du tome II

CHAPITRE 5

1. L'ensemble des sous-ensembles récursifs primitifs de $\mathbb{N}$ étant clos par union finie, il suffit de montrer que les ensembles réduits à un élément sont récursifs primitifs. Or la fonction caractéristique de { n } est égale à :

$$\lambda x.((x+1) \dot{-} n)((n+1) \dot{-} x).$$

2. Posons $g(n) = \alpha_2(f(n),f(n+1))$; on a alors :

$$g(0) = \alpha_2(1,1),$$
$$g(n+1) = \alpha_2(\beta_2^2(g(n)),\beta_2^2(g(n)) + \beta_2^1(g(n))),$$

ce qui montre que g est récursive primitive, de même que f qui est égale à $\beta_2^1 o g$.

3. a) Si $\alpha(\sigma) = \alpha(\sigma') = n$, alors σ et σ' ont même longueur $p = \beta_2^1(n)$ et sont égales car $\alpha_p(\sigma) = \alpha_p(\sigma') = \beta_2^2(n)$. L'image de α est l'ensemble $\{ x \; ; \; \beta_2^1(x) \neq 0 \}$ qui est récursif primitif.

b) On vérifie facilement que :

$$\alpha_2(x_1,x_2) < (x_1 + x_2 + 1)^2,$$

et, par récurrence sur p,

$$\alpha_p(x_1,x_2,\dots,x_p) < (x_1 + x_2 + \cdots + x_p + 1)^{2^{p-1}}.$$

Il suffit donc de choisir $g(x) = (x+1)^{2^x}$.

c) Montrons d'abord que la fonction $\psi = \lambda px.\varphi(p,p,x)$ est récursive primitive. En se reportant à la définition des fonctions β_i^j (1.11), on voit qu'elle peut se définir par récurrence par :

$$\psi(0,x) = 0 \; ;$$
$$\psi(1,x) = x \; ;$$
$$\psi(p+1,x) = \beta_2^2(\psi(p,x)).$$

Maintenant, la fonction φ elle-même se définit par récurrence par :

$\varphi(0,i,x) = 0$;
$\varphi(1,i,x) = x$ si $i = 1$, 0 sinon ;
$\varphi(p+1,i,x) = 0$ si $i = 0$ ou si $i > p+1$;
$\varphi(p+1,i,x) = \varphi(p,i,x)$ si $0 < i < p$;
$\varphi(p+1,i,x) = \beta_2^1(\varphi(p,i,x))$ si $p > 0$ et $i = p$;
$\varphi(p+1,i,x) = \psi(p+1,x)$ si $p > 0$ et $i = p+1$.

d) Le fait que γ est une fonction injective se démontre sans peine à partir du théorème d'unicité de la décomposition d'un nombre en facteurs premiers ; quant à son image, c'est l'ensemble :

{ x ; pour tout p inférieur à x et pour tout q inférieur à p, si p et q sont premiers et si p divise x, alors q divise x },
qui est défini par quantifications bornées et opérations booléennes à partir d'ensembles récursifs primitifs ; il est donc récursif primitif.

e) Soit σ une suite finie, et supposons que $\alpha(\sigma) = x$; on peut alors calculer la longueur de σ qui est égale à $p = \beta_2^1(x)$, et on voit que :

$$\gamma(\sigma) = \prod_{i=1}^{i=p-1} \pi(i)^{\varphi(p,i+1,x)+1} ;$$

on peut donc poser $f(x) = \prod_{i=1}^{i=p-1} \pi(i)^{\varphi(p,i+1,x)+1}$, où $p = \beta_2^1(x)$.

Pour la fonction h, on commence par faire la même chose : on définit sans peine deux fonctions récursives primitives $p(x)$ et $\theta(i,x)$ qui sont telles que, si $\sigma = (x_1, x_2, \ldots, x_p)$ est une suite et $\gamma(\sigma) = x$, alors $p(x)$ est égale à la longueur p de x et, pour tout i compris entre 1 et p, $x_i = \theta(i,x)$. On utilise alors la fonction g du b) et on définit h par :

$h(x) = \mu y \leqslant g(x)$ $(\beta_2^1(y) = p(x)$ et, pour tout i compris entre 1 et $p(x)$, $\theta(i,x) = \varphi(p(x),i,y))$.

4. Le nombre e est la somme de la série :

$$1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} + \cdots$$

Posons $e_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} = \frac{\alpha_n}{n!}$ (α_n étant un entier).

Un calcul simple montre que :

$$\frac{1}{(n+1)!} < e - e_n < \frac{1}{n.n!},$$

et on voit alors que $e.n! - \alpha_n$ est strictement compris entre $\frac{1}{n+1}$ et $\frac{1}{n}$, et donc que, si $n > 2$, α_n est la partie entière de $e.n!$. Si p est un entier quelconque, on a :

$$| e.n! - p | > \frac{1}{n+1} \quad \text{et} \quad | e - \frac{p}{n!} | > \frac{1}{(n+1)!}.$$

Soit alors $\frac{p}{q}$ un rationnel positif quelconque ; il peut s'écrire sous la forme $\frac{p'}{q!}$, et donc :

$$(*) \qquad | e - \frac{p}{q} | > \frac{1}{(q+1)!}.$$

Fixons n et posons $q = 10^n + 1$. On va montrer que la n-ème décimale de e_q est égale à la n-ème décimale de e : soit β la partie entière $10^n.e_q$. Il est clair que $\beta < 10^n.e$, et il suffit donc de montrer que $10^n.e$ est inférieur à $\beta + 1$.

Si on suppose le contraire, on voit, d'après l'inégalité (*), que :

$$e - \frac{\beta+1}{10^n} > \frac{1}{q!},$$

et on a déjà vu que :

$$0 < e - e_q < \frac{1}{qq!} < \frac{1}{q!},$$

ce qui contredit la définition de β.

Maintenant, on voit facilement que la fonction $\alpha = \lambda n.\alpha_n$ est récursive primitive, de même que la fonction qui à n fait correspondre la n–ème décimale de $\frac{\alpha(10^n+1)}{(10^n+1)!}$; ceci termine l'exercice.

5. a) On se débarrasse du cas où a_0 est nul (il y a alors au moins un zéro entier ; cette remarque devra aussi être faite pour b)). Dans les autres cas, il est clair qu'un zéro de $P = a_0 + a_1X + \cdots + a_pX^p$ doit être négatif et que, s'il est entier, il doit diviser a_0. On va supposer que p est pair, par exemple (l'autre cas se traite de la même façon) ; on voit alors que P a un zéro dans $\mathbb{Z}$ si et seulement si il existe un nombre $y \in \mathbb{N}$ inférieur ou égal à a_0 tel que

$$a_0 + a_2y^2 + \cdots + a_py^p = a_1y + a_3y^3 + \cdots + a_{p-1}y^{p-1}.$$

L'ensemble E est donc défini par quantification bornée à partir d'un ensemble récursif primitif.

b) Supposons que $y = -\frac{r}{s}$ soit un zéro de P où r et s appartiennent à $\mathbb{N}$, s est non nul et r et s sont premiers entre eux. On voit alors facilement que r doit diviser a_0 et s doit diviser a_p. En supposant toujours que p soit pair, on voit donc que P a un zéro dans $\mathbb{Q}$ si et seulement si il existe un entier r inférieur ou égal à a_0 et un entier s inférieur ou égal à a_p tel que :

$$a_0s^p + a_2s^{p-2}r^2 + \cdots + a_pr^p = a_1s^{p-1}r + a_3s^{p-3}r^3 + \cdots + a_{p-1}sr^{p-1}.$$

c) On construit d'abord deux fonctions récursives primitives $\theta_1(x,y)$ et $\theta_2(x,y)$ telles que si x code la suite $(a_0,a_1,\ldots,a_p)$ (c'est-à-dire si $\Omega(a_0,a_1,\ldots,a_p) = x$), alors :

$$\theta_1(x,y) = \sum_{2i \leqslant x} \delta(2i,x).y^{2i}$$

et

$$\theta_2(x,y) = \sum_{2i+1 \leqslant x} \delta(2i,x).y^{2i+1}.$$

(δ est la fonction définie en 1.12.)

Ces fonctions sont récursives primitives. On utilise ensuite le même raisonnement qu'au a) : $x \in F$ si et seulement si il existe $y \leqslant \delta(0,x)$ tel que $\theta_1(x,y) = \theta_2(x,y)$.

6. La formule F a un modèle de cardinalité n si et seulement si elle a un modèle $\mathfrak{M}$ dont l'ensemble de base est $A_n = \{ 0,1,\ldots,n-1 \}$. Celui-ci sera alors caractérisé par l'interprétation $R \subseteq A_n^2$ du prédicat binaire. On code le modèle par le couple $(n,u(R))$, où $u(R)$ est l'entier défini par

$$u(R) = \prod_{(i,j) \in R} \pi(\alpha_2(i,j)).$$

Il est facile de voir que $u(R)$ est borné par une fonction récursive primitive de n, ($\alpha_2(n,n)!$ par exemple). On voit aussi sans trop de peine que l'ensemble des codes des L-structures finies :

$$M = \{ (n,u) \text{ ; il existe } R \subseteq A_n^2 \text{ tel que } u = u(R) \},$$

est récursif primitif. On va montrer que l'ensemble :

$$U(F) = \{ (n,u(R)) \text{ ; } R \subseteq A_n^2 \text{ et } (A_n,R) \text{ est un modèle de } F \},$$

est récursif primitif. Il s'ensuivra que $n \in Sp(F)$ si et seulement si il existe un entier u inférieur à $\alpha_2(n,n)!$ tel que $(n,u) \in U(F)$, et donc que $Sp(F)$ est récursif primitif.

La formule F est équivalente à une formule de la forme :

$$Q_1Q_2...Q_pB[v_1,v_2,...,v_p],$$

où p est un entier, où, pour i compris entre 1 et p, Q_i représente soit le quantificateur $\exists v_i$ soit le quantificateur $\forall v_i$ et où $B[v_1,v_2,...,v_p]$ est une formule sans quantificateur.

On commence par montrer que si $C[v_1,v_2,...,v_p]$ est une formule sans quantificateur de L (et dont les variables libres sont parmi $v_1, v_2,..., v_p$), alors l'ensemble :

$$X(C) = \{ (n,u(R),a_1,a_2,...,a_p) \; ; \; (A_n,R) \models C[a_1,a_2,...,a_p] \}$$

est récursif primitif. Ceci se fait sans histoire par induction sur la complexité de C : si C est atomique, c'est-à-dire de la forme Rv_iv_j, avec i et j compris entre 1 et p, alors :

$(n,u,a_1,a_2,...,a_p) \in X(C)$ si et seulement si $(n,u) \in M$ et $a_1, a_2, ..., a_p$ sont tous compris entre 0 et $n-1$ et $\pi(\alpha_2(a_i,a_j))$ divise u.

Ensuite, on remarque que $X(C_1 \wedge C_2) = X(C_1) \cap X(C_2)$, $X(C_1 \vee C_2) = X(C_1) \cup X(C_2)$, et que $(n,u,a_1,a_2,...,a_p) \in X(\neg C)$ si et seulement si $(n,u) \in M$, $a_1, a_2, ..., a_p$ sont tous compris entre 0 et $n-1$ et $(n,u,a_1,a_2,...,a_p) \notin X(C)$.

Il en résulte donc que X(B) est récursif primitif. Maintenant, l'ensemble $U(\varphi)$ est défini par

$$(n,q) \in U(F) \text{ si et seulement si } T_1T_2...T_p((n,q,x_1,x_2,...,x_p) \in X(B))$$

où, pour chaque i compris entre 1 et p, T_i est égal à $\exists x_i \leqslant n-1$ si Q_i est le quantificateur $\exists v_i$, et T_i est égal à $\forall x_i \leqslant n-1$ si Q_i est le quantificateur $\forall v_i$. On voit donc que U(F) est récursif primitif.

7. Laissé au lecteur.

8. La machine a autant de bandes que l'on veut, mais seule la première a de l'importance ; aussi nous négligerons les autres. Elle a trois états e_0, e_1 et e_f. Voici sa table :

$M(e_0,d) = (e_0,d, +1)$; $M(e_0,|) = (e_1,b, +1)$;
$M(e_1,|) = (e_0,b, +1)$; $M(e_1,b) = (e_1,b, 0)$;
$M(e_0,b) = (e_f,b,0)$.

9. a) Soit $\mathscr{M}$ une machine à n bandes calculant f ; on va simuler le calcul effectué par $\mathscr{M}$ à l'aide d'une machine $\mathscr{N}$ à 3 bandes de la façon suivante : le calcul se fera en réalité sur la troisième bande ; la suite des cases numéro 1, $n+1$, $2n+1$, etc. de cette bande jouera le rôle de la première bande de $\mathscr{M}$; la suite des cases numéro 2, $n+2$, $2n+2$, etc. jouera le rôle de la deuxième bande, et ainsi de suite. La machine $\mathscr{N}$ doit d'abord recopier le contenu de la première bande sur la troisième en utilisant seulement une case sur n ; puis elle doit simuler le calcul de $\mathscr{M}$. Ensuite elle doit recopier le contenu de la suite des cases numéro 2, $n+2$, $2n+2$, etc. sur la seconde bande ; enfin elle doit effacer la troisième bande. On laisse au lecteur le soin de trouver le nombre exact d'états nécessaires et d'écrire la table de $\mathscr{N}$ s'il le désire.

b) L'ensemble $\mathfrak{M}_n$ est fini !

c) Il suffit de rajouter $p + 1$ nouveaux états $f_0, f_1, \ldots, f_p$ à l'ensemble des états de $\mathcal{M}$. L'état initial de $\mathcal{N}_p$ est f_0 ; lorsque la machine est dans l'état f_i $(0 \leqslant i \leqslant p - 1)$ elle ajoute un bâton sur la première bande et elle passe dans l'état f_{i+1} ; lorsqu'elle est dans l'état f_p elle ramène sa tête en début de bande et passe dans l'état initial de $\mathcal{M}$; $\mathcal{N}_p$ a donc $n + p + 1$ états.

d) Supposons que la fonction Σ soit T-calculable ; alors la fonction $\lambda x.\Sigma(2x + 1) + 1$ l'est aussi, et on peut supposer que c'est par une machine $\mathcal{M}$ ayant 3 bandes et n états. La machine $\mathcal{N}_n$ construite en c) a alors $2n + 1$ états, et, partant de la configuration blanche termine, avec $\Sigma(2n + 1) + 1$ bâtons sur sa seconde bande, ce qui contredit la définition de Σ.

10. Si f est récursive, alors la fonction caractéristique de son graphe G est

$$\chi_G = \lambda xy.(1 \dot{-} [(y \dot{-} f(x)) + (f(x) \dot{-} y)])$$

qui est manifestement récursive. Réciproquement,

$$f(x) = \mu y\ (x,y) \in G,$$

et donc f est récursive si G l'est.

11. a) On laisse le lecteur vérifier que la relation $\ll$ est bien transitive, réflexive, antisymétrique et totale. Si $(a,b,c) \in \mathbb{N}^3$, et $(x,y,z) \ll (a,b,c)$, alors x, y, et z sont tous les trois inférieurs à $\sup(a,b,c)$, ce qui montre que l'ensemble

$$\{ (x,y,z) \in \mathbb{N}^3 \ ; \ (x,y,z) \ll (a,b,c) \}$$

a, au plus, $(\sup(a,b,c) + 1)^3$ éléments.

Soit $(a,b,c) \in \mathbb{N}^3$. On va définir, en distinguant plusieurs cas, un autre élément (a',b',c') de $\mathbb{N}^3$ dont on vérifiera que c'est le successeur immédiat de (a,b,c) ; posons $\sup(a,b,c) = k$:

- si $k > c$, alors $a' = a$, $b' = b$, $c' = c + 1$;
- si $k = c$, $k > b + 1$ et $k > a$, alors $a' = a$, $b' = b + 1$, $c' = c$;
- si $k = c$, $k > b + 1$ et $k = a$, alors $a' = a$, $b' = b + 1$, $c' = 0$;
- si $k = c = b + 1$, alors $a' = a$, $b' = b + 1$, $c' = 0$;
- si $k = c = b$ et $k > a + 1$, alors $a' = a + 1$, $b' = 0$, $c' = c$;
- si $k = c = b = a + 1$, alors $a' = a + 1$, $b' = 0$, $c' = 0$;
- si $k = c = b = a$, alors $a' = 0$, $b' = 0$, $c' = c + 1$.

b) Les fonctions γ_1, γ_2 et γ_3 sont définies simultanément par récurrence comme dans l'exemple 1.13 : $\gamma_1(0) = \gamma_2(0) = \gamma_3(0) = 0$ et $\gamma_1(n + 1)$, $\gamma_2(n + 1)$, $\gamma_3(n + 1)$ sont définis à partir de $\gamma_1(n)$, $\gamma_2(n)$, $\gamma_3(n)$:

- si $\sup(\gamma_1(n),\gamma_2(n),\gamma_3(n)) > \gamma_3(n)$, alors $\gamma_1(n + 1) = \gamma_1(n)$, $\gamma_2(n + 1) = \gamma_2(n)$, $\gamma_3(n + 1) = \gamma_3(n) + 1$;

• si $\sup(\gamma_1(n),\gamma_2(n),\gamma_3(n)) = \gamma_3(n)$, $\gamma_2(n) + 1 < \sup(\gamma_1(n),\gamma_2(n),\gamma_3(n))$, et $\gamma_1(n) < \sup(\gamma_1(n),\gamma_2(n),\gamma_3(n))$ alors $\gamma_1(n + 1) = \gamma_1(n)$, $\gamma_2(n + 1) = \gamma_2(n) + 1$, $\gamma_3(n + 1) = \gamma_3(n)$;

• si $\sup(\gamma_1(n),\gamma_2(n),\gamma_3(n)) = \gamma_3(n)$, $\gamma_2(n) + 1 < \sup(\gamma_1(n),\gamma_2(n),\gamma_3(n))$, et $\gamma_1(n) = \sup(\gamma_1(n),\gamma_2(n),\gamma_3(n))$ alors $\gamma_1(n + 1) = \gamma_1(n)$, $\gamma_2(n + 1) = \gamma_2(n) + 1$, $\gamma_3(n + 1) = 0$;

• si $\sup(\gamma_1(n),\gamma_2(n),\gamma_3(n)) = \gamma_3(n) = \gamma_2(n) + 1$, alors $\gamma_1(n + 1) = \gamma_1(n)$, $\gamma_2(n + 1) = \gamma_2(n) + 1$, $\gamma_3(n + 1) = 0$;

• si $\sup(\gamma_1(n),\gamma_2(n),\gamma_3(n)) = \gamma_3(n) = \gamma_2(n)$ et $\gamma_1(n) + 1 < \sup(\gamma_1(n),\gamma_2(n),\gamma_3(n))$, alors $\gamma_1(n + 1) = \gamma_1(n) + 1$, $\gamma_2(n + 1) = 0$, $\gamma_3(n + 1) = \gamma_3(n)$;

• si $\sup(\gamma_1(n),\gamma_2(n),\gamma_3(n)) = \gamma_3(n) = \gamma_2(n) = \gamma_1(n) + 1$, alors $\gamma_1(n + 1) = \gamma_1(n) + 1$, $\gamma_2(n + 1) = \gamma_3(n + 1) = 0$;

• si $\sup(\gamma_1(n),\gamma_2(n),\gamma_3(n)) = \gamma_3(n) = \gamma_2(n) = \gamma_1(n)$, alors $\gamma_1(n+1) = \gamma_2(n+1) = 0$, $\gamma_3(n + 1) = \gamma_3(n) + 1$.

Il est clair que $(0,0,0) = (\gamma_1(0),\gamma_2(0),\gamma_3(0))$ est l'élément minimum de $\mathbb{N}^3$ pour la relation $\ll$. D'autre part, en comparant avec ce qui a été dit au a), on voit que, pour tout n, $(\gamma_1(n + 1),\gamma_2(n + 1),\gamma_3(n + 1))$ est le successeur immédiat, pour la relation $\ll$, de $(\gamma_1(n),\gamma_2(n),\gamma_3(n))$.

Pour tout entier n, on voit alors par récurrence sur $p \geqslant 0$, que :

$$(\gamma_1(n + p),\gamma_2(n + p),\gamma_3(n + p)) \gg (\gamma_1(n),\gamma_2(n),\gamma_3(n))$$

et que l'inégalité est stricte si $p > 0$. Ceci montre bien que, pour tous m, n,

$$(\gamma_1(m),\gamma_2(m),\gamma_3(m)) \ll (\gamma_1(n),\gamma_2(n),\gamma_3(n)) \text{ si et seulement si } m \leqslant n,$$

et que, si $m < n$, alors l'inégalité $(\gamma_1(m),\gamma_2(m),\gamma_3(m)) \ll (\gamma_1(n),\gamma_2(n),\gamma_3(n))$ est stricte : l'application $\Gamma = \lambda n.(\gamma_1(n),\gamma_2(n),\gamma_3(n))$ est injective.

Passons à la surjectivité. Soit $(a,b,c) \in \mathbb{N}^3$, et posons $d = \sup(a,b,c)$. On raisonne par l'absurde et on suppose que pour tout $n < (d + 1)^3$, $\Gamma(n) \neq (a,b,c)$. On va alors montrer, par récurrence, que, pour tout $n \leqslant (d + 1)^3$:

$$(\gamma_1(n),\gamma_2(n),\gamma_3(n)) \ll (a,b,c).$$

C'est vrai pour 0, puisque $(\gamma_1(0),\gamma_2(0),\gamma_3(0)) = (0,0,0)$ est le minimum pour la relation $\ll$. Si on suppose que c'est vrai pour n, comme par hypothèse, $(\gamma_1(n),\gamma_2(n),\gamma_3(n)) \neq (a,b,c)$, on voit que $(\gamma_1(n),\gamma_2(n),\gamma_3(n))$ est strictement inférieur, pour l'ordre $\ll$, à (a,b,c), et puisque $(\gamma_1(n+1),\gamma_2(n + 1),\gamma_3(n + 1))$ est le successeur immédiat de $(\gamma_1(n),\gamma_2(n),\gamma_3(n))$, on en déduit :

$$(\gamma_1(n + 1),\gamma_2(n + 1),\gamma_3(n + 1)) \ll (a,b,c).$$

On voit donc que l'ensemble $\{ (x,y,z) ; (x,y,z) \ll (a,b,c) \}$ possède au moins $(d + 1)^3 + 1$ éléments ce qui est impossible puisqu'on a vu au a) que ce dernier ensemble a, au plus, $(d + 1)^3$ éléments.

c) Le fait que H soit un ensemble récursif primitif n'est pas complètement clair : pour calculer $\chi_H(n)$, il faut avoir à sa disposition toutes les valeurs $\chi_H(p)$ pour $p < n$ (et

pas seulement $\chi_H(n-1)$ comme dans une récurrence habituelle). On se reportera à la solution de l'exercice 13 pour voir comment procéder.

Passons maintenant à l'équivalence :

$$n \in H \text{ si et seulement si } \gamma_1(n) = \xi(\gamma_2(n), \gamma_3(n)).$$

Elle se montre par récurrence sur n. Pour $n = 0$, elle est vérifiée puisque $0 \notin H$ et que $\gamma_1(0) = \gamma_2(0) = \gamma_3(0) = 0$ et $\xi(\gamma_2(0), \gamma_1(0)) = 1$. Pour $n \neq 0$, on distingue plusieurs cas :

- si $\gamma_2(n) = 0$, alors l'équivalence se déduit sans difficultés des définitions ;
- même chose si $\gamma_3(n) = 0$;
- plaçons-nous dans l'autre cas ; posons $z = \gamma_1(n)$, $y = \gamma_2(n)$ et $x = \gamma_3(n)$. On suppose d'abord que $z = \xi(y,x)$ et on veut en déduire que $n \in H$. Par définition de la fonction d'Ackermann,

$$z = \xi(y-1, \xi(y, x-1)).$$

Puisque Γ est bijective, il existe deux entiers p et q tels que :

$\gamma_1(p) = \xi(y, x-1)$, $\gamma_2(p) = y$ et $\gamma_3(p) = x-1$

et $\gamma_1(q) = z$, $\gamma_2(q) = y-1$ et $\gamma_3(q) = \gamma_1(p)$.

Des propriétés de la fonction d'Ackermann, il découle facilement que :

$(\gamma_1(p), \gamma_2(p), \gamma_3(p) \ll (\gamma_1(n), \gamma_2(n), \gamma_3(n))$ et $(\gamma_1(q), \gamma_2(q), \gamma_3(q)) \ll (\gamma_1(n), \gamma_2(n), \gamma_3(n))$

et $(\gamma_1(p), \gamma_2(p), \gamma_3(p) \neq (\gamma_1(n), \gamma_2(n), \gamma_3(n))$ et $(\gamma_1(q), \gamma_2(q), \gamma_3(q)) \neq (\gamma_1(n), \gamma_2(n), \gamma_3(n))$,

et donc, $p < n$ et $q < n$; par hypothèse de récurrence, p et q appartiennent à H. La définition récursive de H montre alors que n aussi appartient à H.

Réciproquement, supposons que $n \in H$, et considérons les entiers p et q dont il est question dans la définition récursive de H. Par hypothèse de récurrence, on voit alors que $\gamma_1(p) = \xi(y, x-1)$ et $z = \xi(y-1, \gamma_1(p))$, et cela implique bien que $z = \xi(y,x)$.

d) D'après ce que l'on a vu, $(y,x,z) \in G$ si et seulement si il existe $n \leqslant (\sup(x,y,z)+1)^3$ tel que $n \in H$ et $\gamma_1(n) = z$, $\gamma_2(n) = y$ et $\gamma_3(n) = x$: la fonction d'Ackermann est récursive (exercice 10).

12. Soit $f \in \mathfrak{F}_1$ une fonction récursive croissante ; si f est bornée, son image est finie et donc récursive. Sinon, définissons la fonction g par :

$$g(x) = \mu y\ f(y) \geqslant x \ ;$$

g est alors une fonction récursive totale, et $x \in \mathrm{Im}(f)$ si et seulement si $f(g(x)) = x$.

Soit maintenant $A \subseteq \mathbb{N}$ un ensemble récursif infini ; on définit la fonction f par récurrence :

$f(0) = \mu y\ y \in A$;

$f(n+1) = \mu y\ (y \in A \text{ et } y > f(n))$;

f est récursive, strictement croissante et son image est A.

13. La fonction g sera définie comme suit :

$g(0) = f(0)$;

$g(n + 1) = f(p)$ où p est le plus petit entier tel que $f(p) \notin \{ g(0),g(1),...,g(n) \}$.

Il est à peu près clair que g est une fonction totale injective et que son image est égale à celle de f ; il n'est pas complètement évident qu'elle soit récursive, car pour calculer $g(n + 1)$, il faut connaître toutes les valeurs $g(i)$ pour $i \leqslant n$, et non pas seulement $g(n)$ comme dans une récurrence classique. On va donc commencer par définir la fonction $h(x) = \prod_{t=0}^{t=x} \pi(g(t))$ par la récurrence suivante qui, elle, est tout-à-fait orthodoxe :

$h(0) = \pi(f(0))$;

$h(n + 1) = h(n).\pi(f(\mu y(\pi(f(y))$ ne divise pas $h(n)))))$.

La fonction g se définit alors facilement par $g(0) = f(0)$ et

$g(n + 1) = \mu y(\pi(y)$ divise $h(n + 1)$ mais ne divise pas $h(n))$.

On a vu dans le cours (4.5 et 4.7) qu'il existe des fonctions récursives dont l'image n'est pas récursive. Il en existe donc aussi qui, de plus, sont injectives.

14. Soit A un sous-ensemble récursivement énumérable infini de $\mathbb{N}^p$; on veut montrer qu'il contient un ensemble récursif infini. En remplaçant A par son image par α_p (voir 1.11), on se ramène au cas où $A \subseteq \mathbb{N}$. On sait alors que A est l'image d'une fonction récursive primitive $f \in \mathfrak{F}_1$. On définit la fonction $g \in \mathfrak{F}_1$ par :

$g(0) = f(0)$;

$g(n + 1) = \sup(g(n),f(n + 1))$;

g est une fonction récursive primitive croissante dont l'image est infinie et incluse dans A. Cette image est récursive d'après l'exercice 12.

15. a) L'ensemble B est la projection d'un ensemble récursif : il est donc récursivement énumérable. Montrons que, pour tout $x_0 \in \mathbb{N}$, il existe $x_1 \in \mathbb{N}$, $x_1 > x_0$ et $x_1 \notin B$: il suffit de choisir $x_1 > x_0$ tel que $\alpha(x_1)$ soit minimum dans l'ensemble $\{ \alpha(y) ; y > x_0 \}$.

b) Il est clair que A est récursivement énumérable ; il suffit donc de montrer que, sous les conditions de b), le complémentaire de A est récursivement énumérable (voir 4.2). Puisque C est inclus dans le complémentaire de B, si $x \in C$ et si $y > x$, alors $\alpha(y) > \alpha(x)$; donc α est strictement croissante sur C. Puisque C est infini, l'ensemble $\{ \alpha(x) ; x \in C \}$ n'est pas borné. Soient t un entier et x_0 un élément de C tels que $\alpha(x_0) > t$. Alors t est dans A si et seulement si il existe $y < x_0$ tel que $\alpha(y) = t$. Autrement dit :

$t \notin A$ si et seulement si il existe $x \in C$ tel que $\alpha(x) > t$ et, pour tout $y < x$, $\alpha(y) \neq t$,

et on voit que le complémentaire de A est la projection d'un ensemble récursivement énumérable.

c) Soit A un sous-ensemble infini de $\mathbb{N}$ qui est récursivement énumérable mais pas récursif ; c'est l'image d'une fonction totale récursive, donc, d'après l'exercice 13, c'est

aussi l'image d'une fonction récursive injective que l'on appellera α. Si on pose
$$B = \{ x \text{ ; il existe } y > x \text{ tel que } \alpha(y) < \alpha(x) \}$$
et $D = \mathbb{N} - B$, on voit que B est récursivement énumérable et que D est infini (question a)). Mais D ne peut pas contenir de sous-ensemble récursivement énumérable infini, car alors A serait récursif (question b)). On en déduit que tout ensemble récursivement énumérable infini a une intersection non vide avec B.

16. a) L'ensemble des bijections muni de l'opération de composition est un groupe ; il suffit de montrer que les bijections récursives en forment un sous-groupe, et pour cela il faut montrer que l'idendité est récursive, ce qui est évident, que la composée de deux bijections récursives est récursive, ce qui est encore évident, et que la réciproque d'une bijection récursive est récursive, ce qui n'est pas bien difficile : si f est une bijection, f^{-1} est définie par
$$f^{-1}(x) = \mu y(f(y) = x).$$

b) Rappelons que l'ensemble $C^1 \subseteq \mathbb{N}^4$, défini par : $(i,t,x,y) \in C^1$ si et seulement si la machine d'indice i qui a démarré avec x sur sa première bande a terminé son calcul au temps t et il y a y bâtons inscrits sur sa deuxième bande, est récursif primitif. Si on suppose que f est récursive primitive et que, pour tout x, $f(x) \geqslant T(x)$, alors
$$\varphi(x) = \mu y \leqslant ST^1(e,f(x),x)\ ((e,f(x),x,y) \in C^1)$$
est récursive primitive, ce qui est contraire aux hypothèses.

Le graphe G de T est défini par :

$(x,y) \in G$ si et seulement si $(e,y,x) \in B^1$ et, pour tout $z < y$, $(e,z,x) \notin B^1$,

ce qui montre bien qu'il est récursif primitif.

c) Le fait que g soit récursive et strictement croissante est à peu près évident. Comme $g(x) \geqslant T(x)$ pour tout x, elle n'est pas récursive primitive d'après la question a).

Son graphe G_1 et son image I sont récursifs primitifs car :

- $(x,y) \in G_1$ si et seulement si il existe $i \leqslant x$ tel que $(i,y-2x) \in G$ et, pour tout $j \leqslant x$, il existe $z \leqslant y - 2x$ tel que $(j,z) \in G$.
- $y \in I$ si et seulement si il existe $x \leqslant y$ tel que $(x,y) \in G_1$.

d) On n'a pas le choix : $g'(n)$ doit être le $(n+1)$-ème élément de $\mathbb{N} - I$; comme 0 n'appartient visiblement pas à I (il faut au moins une étape pour effectuer un calcul), il faut poser $g'(0) = 0$. D'autre part, pour tout n, l'ensemble $I \cap \{ y \text{ ; } y \leqslant 2n \}$ a au plus n éléments, donc l'ensemble $(\mathbb{N} - I) \cap \{ y \text{ ; } y \leqslant 2n \}$ en a au moins $n + 1$, ce qui prouve que $g'(n) \leqslant 2n$, et ce qui nous permet de terminer la définition de g' par récurrence :
$$g'(n+1) = \mu y \leqslant 2n+2\ (y \notin I \text{ et } y > g'(n)).$$

e) Il est clair, d'après sa définition, que la fonction h est récursive, injective et surjective. On voit aussi qu'elle ne peut pas être récursive primitive sinon g le serait aussi. Maintenant h^{-1} peut être définie de la façon suivante :

$h^{-1}(x) = 2(\mu y \leqslant x\ ((y,x) \in G_1))$ si $x \in I$;
$h^{-1}(x) = 2(\mu y \leqslant x\ (g'(y) = x)) + 1$ sinon,

ce qui montre que h^{-1} est récursive primitive. En revanche, on vient de voir que h, sa réciproque, ne l'est pas.

17. Prenons un ensemble $B' \subseteq \mathbb{N}$ récursivement énumérable non récursif (le domaine de définition de la fonction partielle $\lambda x.\varphi^1(x,x)$, par exemple) ; il existe un ensemble récursif C dont B' est la projection :

$$B' = \{ x \text{ , il existe } y \in \mathbb{N} \text{ tel que } (x,y) \in C \}.$$

Le complémentaire A de C est aussi récursif et

$$B = \mathbb{N} - B' = \{ x \text{ ; pour tout } y \in \mathbb{N}, (x,y) \in A \}$$

n'est pas récursivement énumérable, sinon B' serait récursif (4.2).

18. Considérons la fonction partielle $g \in \mathfrak{F}_2^*$ définie par :

$$g(x,t) = \mu y\ (\varphi^1(x,y) = t).$$

Elle est récursive et, si φ^1_x est une bijection de $\mathbb{N}$ dans $\mathbb{N}$, alors $\lambda t.g(x,t)$ est la bijection réciproque. Soit i un indice de g ; on a donc, pour tous x et t :

$$g(x,t) = \varphi^2(i,x,t).$$

En appliquant maintenant le théorème smn on obtient :

$$g(x,t) = \varphi^1(s^1_1(i,x),t),$$

et on voit qu'un indice de la bijection réciproque de φ^1_x est $s^1_1(i,x)$. On peut donc prendre pour α la fonction $\lambda x.s^1_1(i,x)$, qui est récursive primitive.

19. Définissons :

$$f_0 = g,$$

et, par récurrence sur x,

$$f_{x+1}(y) = h(f_x(\alpha(y)),y,x)$$

Il est alors clair que la fonction partielle $\lambda xy.f_x(y)$ est l'unique fonction partielle qui satisfasse les conditions de l'énoncé. Il est aussi évident que chacune des f_x est récursive, mais il n'est pas clair, a priori, que f elle-même le soit. Pour le montrer, on va copier la démonstration qui a permis de montrer que la fonction d'Ackermann est récursive.

Considérons l'application qui, à chaque fonction partielle $k \in \mathfrak{F}_2^*$, fait correspondre $k^* \in \mathfrak{F}_2^*$ définie par :

$k^*(0,y) = g(y)$;
$k^*(x + 1,y) = h(k(x,\alpha(y)),y,x)$.

On remarque que f est la seule fonction partielle qui satisfasse $f^* = f$. D'autre part, comme dans le cas de la fonction d'Ackermann, on trouve, en utilisant le théorème smn, une fonction récursive primitive β telle que, si $k = \varphi^2_x$ alors $k^* = \varphi^2_{\beta(x)}$. Le théorème du point fixe nous apprend qu'il existe un entier i tel que $\varphi^2_i = \varphi^2_{\beta(i)}$, et donc f est égale à φ^2_i et est récursive.

20. Si la fonction $\lambda x.T^1(i,x)$ peut être prolongée en une fonction totale récursive h, alors A est récursif : pour savoir si $n \in A$, on regarde si la machine d'indice i a terminé son calcul après h(n) étapes.

21. a) Pour montrer qu'une fonction récursive primitive est calculable en un temps récursif primitif, il suffit de reprendre la démonstration du fait que toute fonction partielle récursive est T-calculable ; si on n'utilise pas le schéma μ, comme c'est le cas lorsqu'on a affaire à une fonction récursive primitive, on s'aperçoit que l'on peut borner le temps de calcul par une fonction récursive primitive.

La réciproque est exactement la première remarque faite en 3.14.

b) Découle du corollaire 2.4.

c) Lorsque l'on fixe n (et A et i), la fonction $\lambda x.\xi(n,x)$ est récursive primitive, de même que la fonction $\lambda x.g(i,A,n,x)$. Réciproquement, supposons que $f \in \mathfrak{F}_1$ soit récursive primitive. Alors, d'après a) et b), il existe des entiers i, n et A tels que f(x) soit calculée par la machine d'indice i en un temps qui est borné par $\sup(A,\xi(n,x))$. Autrement dit :

$$f = \lambda x.g(i,A,n,x).$$

d) On voit donc que l'ensemble des fonctions $\lambda x.g(i,A,n,x)$, où i, A et n sont des entiers, est égal à l'ensemble de toutes les fonctions récursives primitives à une variable. On obtient la fonction cherchée en posant :

$$\psi(x,y) = g(\beta_3^1(x),\beta_3^2(x),\beta_3^3(x),y).$$

e) On utilise un argument diagonal : l'ensemble

$$X = \{ x \ ; \ \psi(x,x) = 0 \}$$

est manifestement récursif. Il n'est pas récursif primitif, car, s'il l'était, il existerait un entier y tel que sa fonction caractéristique soit égale à $\lambda x.\psi(y,x)$ et on en déduirait que :

$$y \in X \text{ si et seulement si } y \notin X,$$

ce qui est absurde.

22. a) C'est toujours le même argument diagonal : si on suppose que l'ensemble des fonctions totales récursives à une variable est énuméré au moyen de la fonction F(x,y), on obtient une contradiction en considérant la fonction $\lambda x.F(x,x) + 1$.

b) Soit F(x,y) une fonction récursive énumérant les fonctions récursives primitives à une variable (exercice 21). On définit G(x,y) par :

$$G(x,0) = F(x,0) \ ;$$
$$G(x,y+1) = \sup(G(x,y) + 1, F(x,y+1)).$$

On vérifie que, pour tout x, la fonction $G_x = \lambda y.G(x,y)$ est récursive primitive et strictement croissante, et que, de plus, si F_x est elle même strictement croissante, $G_x = F_x$. L'ensemble $\{ G_x \ ; \ x \in \mathbb{N} \}$ est donc bien égal à l'ensemble de toutes les fonctions récursives primitives strictement croissantes à une variable.

c) On utilise la même technique : on définit la fonction H par

$H(x,0) = F(x,0)$;

$H(x,y+1) = F(x,y+1)$ si $F(x,y+1) \notin \{ H(x,t) \; ; \; 0 \leqslant t \leqslant y \}$;

$H(x,y+1) = \sup \{ H(x,i) + 1 \; ; \; 0 \leqslant i \leqslant y \}$ sinon.

(Pour montrer que la fonction H est récursive et que les fonctions H_x sont toutes récursives primitives, il faut utiliser la technique indiquée dans la solution de l'exercice 13).

d) On va construire une fonction g récursive strictement croissante, dont l'image B ne contient aucun des ensembles A_x ; B sera un ensemble récursif d'après l'exercice 12, ce qui répondra à la question. On définit g par :

$g(0) = 0$

$g(x+1) = \beta_2^2(\mu t[\beta_2^2(t) = F(x,\beta_2^1(t))$ et $\beta_2^2(t) > g(x)] + 1$.

La fonction g est manifestement récursive, et le fait que l'image de $\lambda y.F(x,y)$ est infinie entraîne qu'elle est totale.

Pour tout entier x, posons : $a = (\mu t[\beta_2^2(t) = F(x,\beta_2^1(t))$ et $\beta_2^2(t) > g(x)]$, $b = \beta_2^2(a)$, $c = \beta_2^1(a)$. On a alors :

$g(x+1) = b + 1$, $b > g(x)$ et $b = F(x,c)$.

Cela montre que g est strictement croissante et que b qui appartient à l'image de la fonction $\lambda y.F(x,y)$ (c'est-à-dire à A_x), est strictement compris entre $g(x)$ et $g(x+1)$ et n'appartient donc pas à l'image de g.

Si l'ensemble des fonctions récursives strictement croissantes ou des fonctions récursives injectives était récursivement énuméré, il le serait à l'aide d'une fonction $F \in \mathfrak{F}_2$ telle que, pour tout entier x, l'image de $\lambda y.F(x,y)$ est infinie : on vient de construire une fonction g récursive strictement croissante, donc injective, ne pouvant être égale à aucune des fonctions $\lambda y.F(x,y)$.

23 a) Immédiat à partir du fait que l'ensemble des fonctions récursives totales contient la fonction identité et est clos par composition.

b) Supposons que B soit un ensemble récursivement énumérable : c'est donc le domaine de définition d'une fonction partielle récursive h. Maintenant, si A est réductible à B, c'est qu'il existe une fonction récursive f telle que :

si $x \in A$ alors $f(x) \in B$ et donc $h \circ f(x)$ est défini ;

si $x \notin A$ alors $f(x) \notin B$ et donc $h \circ f(x)$ n'est pas défini ;

cela montre que A est le domaine de définition de $h \circ f$ et qu'il est donc récursivement énumérable.

Il est bien clair que $A \leqslant B$ si et seulement si $\mathbb{N} - A \leqslant \mathbb{N} - B$. Donc, si on suppose que B est récursif, alors A et $\mathbb{N} - A$ sont tous les deux récursivement énumérables, et donc A est récursif.

c) On sait que Y est récursivement énumérable ; donc, avec le résultat du b), on voit que, si $A \leqslant Y$, alors A est récursivement énumérable. Réciproquement, supposons que A soit le domaine de définition de la fonction partielle récursive d'indice e. Alors $x \in A$ si et seulement si $\varphi^1(e,x)$ est défini, si et seulement si $\alpha_2(e,x) \in Y$: A est réductible à Y.

d) Il est d'abord bien clair que A et B sont tous deux réductibles à C : $x \in A$ si et seulement si $2x \in C$, et $x \in B$ si et seulement si $2x + 1 \in C$.

Soient $D \subseteq \mathbb{N}$ et f et g deux fonctions telles que :

$$x \in A \text{ si et seulement si } f(x) \in D,$$

et

$$x \in B \text{ si et seulement si } g(x) \in D.$$

Il s'agit de montrer que C est réductible à D. Il suffit de considérer la fonction h définie par :

$$h(x) = f(x/2) \text{ si x est pair ;}$$
$$h(x) = g(\frac{x-1}{2}) \text{ si x est impair ;}$$

et on voit alors facilement que $x \in C$ si et seulement si $h(x) \in D$.

e) Soit $B \subseteq \mathbb{N}$; appliquons la construction du d) aux ensembles B et $\mathbb{N} - B$, et on obtient un ensemble C. On va montrer que C est autodual : puisque B et $\mathbb{N}$ - B sont tous deux réductibles à C, on voit que $\mathbb{N} - B$ et B sont réductibles à $\mathbb{N} - C$. Il découle de la propriété de minimalité de C démontrée en d) que C est réductible à $\mathbb{N} - C$.

f) *i*) Soit f une fonction partielle récursive n'appartenant pas à $\mathcal{F}$; considérons la fonction $\theta(x,y) = f(y) + \varphi^1(x,x) - \varphi^1(x,x)$, et posons, pour chaque entier n :

$$\theta_n = \lambda y.\theta(n,y) ;$$

θ_n est donc la fonction partielle de domaine vide si $n \in \mathbb{N} - X$, et est égale à f sinon. Si e est un indice pour θ, le théorème smn nous dit que $s_1^1(e,n)$ est un indice pour θ_n. On voit que $n \in \mathbb{N} - X$ si et seulement si $s_1^1(e,n) \in A$, ce qui montre que $\mathbb{N} - X$ est réductible à A donc X à $\mathbb{N} - A$.

ii) On va choisir maintenant une fonction partielle récursive f appartenant à $\mathcal{F}$, et on pose encore $\theta(x,y) = f(y) + \varphi^1(x,x) - \varphi^1(x,x)$ et, pour chaque entier n, $\theta_n = \lambda y.\theta(n,y)$. Si e est un indice de θ, $s_1^1(e,n)$ est un indice de θ_n ; alors, $n \in X$ si et seulement si $s_1^1(e,n) \in A$, et X est réductible à A.

iii) On raisonne par l'absurde et on suppose qu'il existe une fonction récursive f telle que pour tout entier x, $x \in A$ si et seulement si $f(x) \in \mathbb{N} - A$. Le premier théorème du point fixe fournit un entier n tel que $\varphi_n^1 = \varphi_{f(n)}^1$, donc tel que $n \in A$ si et seulement si $f(n) \in A$, ce qui est contradictoire.

g) Pour montrer que Y est réductible à X, considérons la fonction partielle :

$$\psi(x,y) = \varphi^1(\beta_2^1(x),\beta_2^2(x)),$$

et pour chaque entier n posons $\psi_n = \lambda y.\psi(n,y)$. Cette fonction partielle est totale (et

constante) si $n \in Y$ et n'est jamais définie sinon ; d'autre part, si e est un indice pour ψ, $s_1^1(e,n)$ est un indice pour ψ_n. Donc, si $n \in Y$, alors $\varphi^1(s_1^1(e,n),s_1^1(e,n))$ est défini et $s_1^1(e,n) \in X$. Réciproquement si $n \notin Y$, alors $\varphi^1(s_1^1(e,n),s_1^1(e,n))$ n'est pas défini et $s_1^1(e,n) \notin X$, ce qui montre que $Y \leqslant X$.

24. Le fait que ψ soit une fonction partielle récursive provient de ce qu'elle a été définie par cas, comme cela nous a été permis en 4.6. On voit aussi que $g(x) = 0$ si $\varphi^1(x,0)$ est défini, et $g(x) = 1$ sinon. Autrement dit, g est la fonction caractéristique de l'ensemble :

$$\{ x ; \varphi^1(x,0) \text{ n'est pas défini } \},$$

qui n'est pas récursif d'après le théorème de Rice : g n'est pas récursive.

25. a) Tout d'abord, A est le domaine de définition de la fonction partielle récursive $\lambda x.\varphi^1(x,0)$; c'est donc un ensemble récursivement énumérable. Considérons l'ensemble :

$$\mathscr{A} = \{ f ; f \in \mathfrak{F}_1^* , \text{ f est récursive et } f(0) \text{ est défini } \} ;$$

il est bien clair que $\mathscr{A}$ n'est ni vide, ni l'ensemble de toutes les fonctions partielles récursives à une variable, et le théorème de Rice permet donc de conclure que A n'est pas récursif. Comme on sait déjà que A est récursivement énumérable, on en déduit que son complémentaire n'est pas récursivement énumérable (4.2).

b) Considérons la fonction partielle $H = \lambda xy.sg(1 + \varphi^1(x,0))$; elle est récursive, et elle possède donc un indice a :

$$H = \varphi_a^2.$$

Pour chaque entier n, considérons maintenant la fonction $H_n = \lambda y.H(n,y)$. Le théoréme smn nous dit que $s_1^1(a,n)$ est un indice de H_n, et, d'autre part, on voit facilement que si $n \in A$, alors H_n est la fonction constante égale à 1, tandis que si $n \notin A$, H_n est la fonction de domaine vide. Donc :

$$n \in A \text{ si et seulement si } s_1^1(a,n) \in B.$$

On peut donc prendre pour α la fonction récursive primitive $\lambda x.s_1^1(a,x)$.

Le fait que B n'est pas le complémentaire d'un récursivement énumérable découle du petit lemme suivant qui va servir plusieurs fois dans la suite :

LEMME : *Soient* $C \subseteq \mathbb{N}$ *et* $f \in \mathfrak{F}_1$ *une fonction récursive totale et on suppose que, pour tout entier* n,

$$n \in A \textit{ si et seulement si } f(n) \in C ;$$

alors $\mathbb{N} - C$ *n'est pas récursivement énumérable.*

Supposons le contraire, et soit h une fonction partielle récursive dont le domaine est $\mathbb{N} - C$; alors $n \notin A$ si et seulement si $h(f(n))$ est défini, ce qui implique que $\mathbb{N} - A$ est récursivement énumérable (domaine de la fonction $h \circ f$). Or cela est faux.

c) On remarque que, si $n \notin A$, alors $B^1(e,z,n)$ n'est vérifié pour aucune valeur de z, et par conséquent, la fonction $\lambda y.F(n,y)$ est égale à la fonction constante égale à 1. D'un autre côté, si $n \in A$, $B^1(e,z,n)$ est vérifié pour toutes les valeurs de z qui sont supérieures ou égales au temps de calcul de la machine d'indice e travaillant avec l'entier n représenté sur sa première bande à l'instant initial ; la fonction $\lambda y.F(n,y)$ a donc dans ce cas un domaine fini. La fonction F est manifestement récursive : appelons b un indice de F. Alors, par le théorème smn, $s_1^1(b,n)$ est un indice de $\lambda y.F(n,y)$. On voit donc que :

$$n \in A \text{ si et seulement si } s_1^1(e,n) \in \mathbb{N} - B,$$

d'où il découle, par le lemme ci-dessus, que B n'est pas récursivement énumérable.

d) Posons $B' = \{ x \ ; \ \varphi_x^1 = f \}$; pour montrer que ni B' ni son complémentaire ne sont récursivement énumérables, on va construire deux fonctions récursives primitives γ et δ à une variable telles que, pour tout entier n :

$$n \in A \text{ si et seulement si } \gamma(n) \in B' ;$$
$$n \in A \text{ si et seulement si } \delta(n) \in \mathbb{N} - B'.$$

Considérons les fonctions H' et F' définies par :

$$H'(x,y) = f(y).H(x,y) ;$$
$$F'(x,y) = f(y).F(x,y),$$

(où H et F sont les fonctions définies aux questions b) et c)) et soient, respectivement, c et d des indices de ces fonctions. On voit, comme précédemment, que, pour tout entier n, $s_1^1(c,n)$ et $s_1^1(d,n)$ sont des indices pour les fonctions $H_n' = \lambda y.H'(n,y)$ et $F_n' = \lambda y.F'(n,y)$. En utilisant ce que l'on sait sur les fonctions H et F, on voit que, si $n \in A$, alors H_n' est égale à f et F_n' est une fonction de domaine fini (donc différente de f) ; si, au contraire, $n \notin A$, F_n' est égale à f et H_n' est la fonction de domaine vide. On a donc démontré que :

$$n \in A \text{ si et seulement si } s_1^1(c,n) \in B' ;$$
$$n \in A \text{ si et seulement si } s_1^1(d,n) \in \mathbb{N} - B'.$$

La proposition de l'énoncé découle alors du lemme.

26. a) Considérons la fonction $\lambda nx.n$; elle est récursive et il existe donc un entier i tel que, pour tous n et x :

$$\varphi^2(i,n,x) = n,$$

et en posant $\delta = \lambda n.s_1^1(i,n)$, on voit que la fonction $\varphi_{\delta(n)}^1$ est bien la fonction constante égale à n.

b) La troisième version du théorème du point fixe nous dit qu'il existe une fonction récursive primitive h(n,t) telle que, pour tous n et t,

$$\varphi_{h(n,t)}^1 = \varphi_{\gamma(n,t,h(n,t))}^1.$$

Si $h(n,t) \leqslant t$, alors $\gamma(n,t,h(n,t)) = \delta(n)$; sinon $\gamma(n,t,h(n,t)) = t$ et on obtient bien ce que l'on veut.

c) L'application de A_t dans l'ensemble $\{0,1,...,t\}$ qui à n fait correspondre $h(n,t)$ est injective : en effet, si n et m sont dans A_t et $n \neq m$, alors :

$$\varphi^1_{h(n,t)} = \varphi^1_{\delta(n)} \neq \varphi^1_{h(m,t)} = \varphi^1_{\delta(m)},$$

ce qui montre bien que $h(n,t) \neq h(m,t)$, et que A_t n'a pas plus de $t + 1$ éléments. On peut donc définir :

$$\alpha(t) = \mu n \leqslant t + 1\ (h(n,t) > t) \text{ et } \beta(t) = h(\alpha(t),t).$$

Alors $\beta(t) > t$ et $\varphi^1_{\beta(t)} = \varphi^1_{h(\alpha(t),t)} = \varphi^1_t$.

27. a) On montre d'abord que *i*) implique *ii*). La fonction φ^1 est partielle récursive, donc il existe un indice i tel que $\varphi^1 = \psi^2_i$ et donc tel que, pour tous x, y :

$$\varphi^1(x,y) = \psi^2(i,x,y) = \psi^1(\sigma^1_1(i,x),y) = \theta(\sigma^1_1(i,x),y).$$

Il suffit donc de choisir $\beta = \lambda x.\sigma^1_1(i,x)$.

Pour montrer que *ii*) implique *i*), posons :

$$\psi^p(i,x_1,x_2,...,x_p) = \theta(i,\alpha_p(x_1,x_2,...,x_p)).$$

La propriété (énu) est facile à vérifier : soit f une fonction partielle récursive à p variables. Alors la fonction $g = \lambda x.f(\beta^1_p(x),\beta^2_p(x),...,\beta^p_p(x))$ est aussi partielle récursive, et il existe un entier i tel que $g = \theta_i$, et on voit que $f = \psi^p_i$. Passons donc à la propriété (snm) : on sait qu'il existe un entier e tel que $\theta = \varphi^2_e$, et, en posant $\alpha(i) = s^1_1(e,i)$, on voit que $\theta_i = \varphi^1_{\alpha(i)}$; on a :

$$\begin{aligned}\psi^{n+m}(i,x_1,x_2,...,x_n,y_1,y_2,...,y_m) &= \theta(i,\alpha_{n+m}(x_1,x_2,...,x_n,y_1,y_2,...,y_m)) \\ &= \varphi^1(\alpha(i),\alpha_{n+m}(x_1,x_2,...,x_n,y_1,y_2,...,y_m)).\end{aligned}$$

Considérons maintenant la fonction partielle

$$\lambda i x_1 x_2 ... x_n z.\varphi^1(\alpha(i),\alpha_{n+m}(x_1,x_2,...,x_n,\beta^1_m(z),\beta^2_m(z),...,\beta^m_m(z))).$$

Elle a un indice e', et donc, pour tous $i,x_1,x_2,...,x_n$ et z :

$$\begin{aligned}\psi^{n+m}(i,x_1,x_2,...,x_n,\beta^1_m(z),\beta^2_m(z),...,\beta^m_m(z)) &= \varphi^1(\alpha(i),\alpha_{n+m}(x_1,x_2,...,x_n,\beta^1_m(z),\beta^2_m(z),...,\beta^m_m(z))) \\ = \varphi^{n+2}(e',i,x_1,x_2,...,x_n,z) &= \varphi^1(s^1_{n+2}(e',i,x_1,x_2,...,x_n),z) = \theta(\beta(s^1_{n+2}(e',i,x_1,x_2,...,x_n)),z).\end{aligned}$$

En remplaçant z par $\alpha_m(y_1,y_2,...,y_m)$, et en posant

$$\sigma^m_n(i,x_1,x_2,...,x_n) = \beta(s^1_{n+2}(e',i,x_1,x_2,...,x_n)),$$

on obtient :

$$\begin{aligned}\psi^{n+m}(i,x_1,x_2,...,x_n,y_1,y_2,...,y_m) &= \theta(\sigma^m_n(i,x_1,x_2,...,x_n),\alpha_m(y_1,y_2,...,y_m)) = \\ &\psi^m(\sigma^m_n(i,x_1,x_2,...,x_n),y_1,y_2,...,y_m).\end{aligned}$$

b) La démonstration des théorèmes du point fixe qui se trouve dans le cours n'utilise que le théorème d'énumération et le théorème smn : on fait exactement la même démonstration.

c) La fonction α a déjà été construite, et la fonction β est donnée par les hypothèses. Il faut juste voir que l'on peut les supposer injectives. On sait comment faire pour la fonction α : il suffit d'utiliser une fonction $\delta(n,x)$, strictement croissante en sa première variable et telle que, pour tous n et x,

$$\varphi^1_{\delta(n,x)} = \varphi^1_x .$$

Pour la fonction β, on fait le même raisonnement. Il faut donc montrer qu'il existe une fonction $\gamma(n,x)$ telle que, pour tous n et x,

$$\theta_{\gamma(n,x)} = \theta_x,$$

et pour cela, on se sert de la démonstration donnée par l'exercice 26 qui n'utilise que les théorèmes du point fixe et qui peut donc s'appliquer à la famille Ψ.

d) On va utiliser les fonctions δ et γ mentionnées en c). On va construire deux suites de fonctions f_n et g_n pour $n \geqslant -1$, qui seront respectivement des approximations pour les fonctions ε et ε^{-1} que l'on cherche à construire. Plus précisément, on s'apercevra, lorsque la construction sera terminée, que, pour $n \in \mathbb{N}$,

$$f_n(p) = \varepsilon(p) \text{ et } g_n(p) = \varepsilon^{-1}(p) \text{ si } p \leqslant n$$
$$f_n(p) = g_n(p) = 0 \text{ si } p > n.$$

On va s'arranger pour que, de plus, pour tout p inférieur ou égal à n, $\varphi_p = \theta^1_{f_n(p)}$ et $\theta_p = \varphi^1_{g_n(p)}$. Ces fonctions f_n et g_n se définissent simultanément par récurrence sur n. Pour f_{-1} et g_{-1}, on peut prendre les fonctions constantes égales à 0. Voyons le cas $n + 1$:

- $f_{n+1}(p) = f_n(p)$ sauf si $p = n + 1$;
- s'il existe $a \leqslant n$ tel que $g_n(a) = n + 1$, alors on pose $f_{n+1}(n + 1) = a$;
- sinon $f_{n+1}(n + 1)$ est le plus petit entier m n'appartenant pas à l'ensemble (fini) $\{0,1,\ldots,n\} \cup \{f_n(0),f_n(1),\ldots,f_n(n)\}$ (ne pas tenir compte de cette condition si $n = -1$) et tel que m soit égal à $\gamma(k,\beta(n + 1))$ pour un certain entier k.

On définit g_{n+1} de façon analogue :

- $g_{n+1}(p) = g_n(p)$ sauf si $p = n + 1$;
- s'il existe $a \leqslant n + 1$ tel que $f_{n+1}(a) = n + 1$, alors : $g_{n+1}(n + 1) = a$;
- sinon $g_{n+1}(n + 1)$ est le plus petit entier m non nul n'appartennant pas à l'ensemble $\{1,\ldots,n + 1\} \cup \{g_n(0),g_n(1),\ldots,g_n(n)\}$ et tel que m soit égal à $\delta(k,\alpha(n + 1))$ pour un certain entier k.

On laissera au lecteur le soin de vérifier que les fonctions $\lambda nx.f_n(x)$ et $\lambda nx.g_n(x)$ sont récursives, de même que la fonction $\varepsilon = \lambda x.f_x(x)$; la fonction $\lambda x.g_x(x)$ est la fonction réciproque de ε, qui est donc bijective et satisfait bien les propriétés voulues.

CHAPITRE 6

1. a) Il suffit de vérifier les axiomes A_1, A_2, ... et A_7, ce qui n'offre pas grande difficulté. Traitons A_7 à titre d'exemple. Soient donc a et b dans M, et montrons que

(•) $$a \times Sb = (a \times b) + a.$$

Il faut distinguer plusieurs cas :

i) a et b sont tous deux dans $\mathbb{N}$; alors (•) est évident puisque $\mathfrak{M}$ est une extension de $\mathbb{N}$;

ii) $a \in X \times \mathbb{Z}$, disons $a = (x,n)$, et $b \in \mathbb{N}$; alors $Sb = b + 1$, $a \times Sb = (x, n \times (b + 1))$.

– Si $b = 0$, $a \times Sb = (x,n) = a$ et $a \times b = 0$, et on a bien $(a \times b) + a = a \times Sb$;

– Si $b \neq 0$, $a \times b = (x, n \times b)$ et $(a \times b) + a = (x, (n \times b) + n) = a \times Sb$;

iii) $a \in \mathbb{N}$ et $b \in X \times \mathbb{Z}$, disons $b = (y,m)$; alors $Sb = (y, m + 1)$ et $a \times Sb = (y, a \times (m + 1))$. D'autre part, $a \times b = (y, a \times m)$, et $(a \times b) + a = (y, (a \times m) + a)$;

iv) $a \in X \times \mathbb{Z}$ et $b \in X \times \mathbb{Z}$, disons $a = (x,n)$ et $b = (y,m)$; alors $Sb = (y, m + 1)$, $a \times Sb = (f(x,y), n \times (m + 1))$; d'autre part, $a \times b = (f(x,y), n \times m)$ et $a \times b + a = (f(x,y), (n \times m) + n)$.

b) On va se servir de a) pour construire un modèle de $\mathscr{P}_0$ dans lequel aucune des formules données n'est vraie. Il suffit de prendre un ensemble X ayant au moins deux éléments, par exemple $X = \mathbb{N}$ et une fonction f non associative, par exemple $f(x,y) = x + 2y$. Dans le modèle $\mathfrak{M}$ construit en suivant a) à partir de ces données, on a, par exemple :

$$(1,1) + (2,0) = (1,1) \text{ et } (2,0) + (1,1) = (2,1),$$

ce qui montre que l'addition n'est pas commutative, et

$$((1,1) \times (2,2)) \times (3,3) = (5,2) \times (3,3) = (11,6)$$

et $$(1,1) \times ((2,2) \times (3,3)) = (1,1) \times (8,6) = (17,6),$$

ce qui montre que la multiplication n'est pas associative. Pour la troisième formule on voit par exemple que $(1,0) \leqslant (1,1)$ (parce que $(1,1) + (1,0) = (1,1)$)et $(1,1) \leqslant (1,0)$ (parce que $(1,-1) + (1,1) = (1,0)$). La quatrième formule n'est pas vérifiée parce que, par exemple, $0 \times (1,0) = (1,0)$.

c) Dans les modèles que l'on vient de construire, l'addition est associative. Mais on peut utiliser la même idée pour voir que l'associativité de l'addition ne découle pas de $\mathscr{P}_0$. Voici un modèle de $\mathscr{P}_0$, parmi beaucoup d'autres, dans lequel l'addition n'est pas associative : l'ensemble de base est $\mathbb{N} \cup (\mathbb{N} \times \mathbb{Z})$, c'est une extension de $\mathbb{N}$, et S, $+$ $_5$$_4$ $\times$ sont interprétés de la façon suivante :

$$S(n,a) = (n,a+1) ;$$
$$(n,a) + m = (n,a+m) = m + (n,a) ;$$
$$(n,a) + (m,b) = (n+2m,a+b) \text{ si } n \neq m \quad \text{et} \quad (n,a) + (n,b) = (n,a+b) ;$$

$(n,a) \times m = (n,am) = m \times (n,a)$ si $m \neq 0$ et $(n,a) \times 0 = 0 \times (n,a) = 0$;
$(n,a) \times (m,b) = (2nb,ab)$.

Là encore, il n'y a aucune difficulté à montrer que les sept axiomes de $\mathscr{P}_0$ sont vérifiés et, par exemple :

$$((1,0) + (2,0)) + (3,0) = (11,0) ;$$
$$(1,0) + ((2,0) + (3,0)) = (17,0).$$

2. a) Il est clair que la relation $\approx$ est symétrique ; elle est réflexive à cause de l'axiome A_4. Voyons la transitivité : si x, y et z sont des éléments de $\mathfrak{M}$ et s'il existe des entiers n, m, p et q tels que :

$$\mathfrak{M} \models x \underline{+} \underline{n} \simeq y \underline{+} \underline{m} \text{ et } \mathfrak{M} \models y \underline{+} \underline{p} \simeq z \underline{+} \underline{q} ;$$

alors, parce que l'addition est associative et commutative dans tous les modèles de $\mathscr{P}$:

$$\mathfrak{M} \models x \underline{+} \underline{n+p} \simeq z \underline{+} \underline{m+q}.$$

b) Par hypothèse, on a des entiers n, m, p et q tels que :

$$\mathfrak{M} \models a \underline{+} \underline{n} \simeq a' \underline{+} \underline{m} \text{ et } \mathfrak{M} \models b \underline{+} \underline{p} \simeq b' \underline{+} \underline{q}$$

et, parce que l'addition est associative et commutative dans tout modèle de $\mathscr{P}$:

$$\mathfrak{M} \models (a \underline{+} b) \underline{+} \underline{n+p} \simeq (a' \underline{+} b') \underline{+} \underline{m+q} .$$

c) La réflexivité est évidente. Montrons la transitivité : on suppose donc que x, y et z sont dans E et que xRy et yRz. Il existe donc a, b et c respectivement dans x, y et z tels que :

$$\mathfrak{M} \models a \leqslant b \wedge b \leqslant c ;$$

donc, parce que $\leqslant$ est une relation d'ordre dans tout modèle de $\mathscr{P}$,

$$\mathfrak{M} \models a \leqslant c.$$

Voyons maintenant que R est antisymétrique : on suppose qu'il y a des points a et a' dans $x \in E$ et b et b' dans $y \in E$ tels que :

$$\mathfrak{M} \models a \leqslant b \text{ et } \mathfrak{M} \models b' \leqslant a' .$$

Il s'agit de montrer que $x = y$. On traduit les hypothèses : il existe u et v dans $\mathfrak{M}$ et des entiers n, m, p et q tels que :

$$\mathfrak{M} \models a \underline{+} u \simeq b \;\; ; \mathfrak{M} \models b' \underline{+} v \simeq a' \;\; ; \mathfrak{M} \models a \underline{+} \underline{n} \simeq a' \underline{+} \underline{m} \;\; ; \mathfrak{M} \models b \underline{+} \underline{p} \simeq b' \underline{+} \underline{q} .$$

Tout ceci, en utilisant l'associativité et la commutativité de l'addition, donne :

$$\mathfrak{M} \models a \underline{+} u \underline{+} v \underline{+} \underline{p+m} \simeq a \underline{+} \underline{n+q} .$$

De la propriété (19) de 1.4, on déduit que $\mathfrak{M} \models u \leqslant \underline{n+q}$, et parce que $\mathbb{N}$ est un segment initial de $\mathfrak{M}$, $u \in \mathbb{N}$ et $a \approx b$. Ainsi, $x = y$.

L'ordre R est bien total : si x et y sont des éléments de E, si $a \in x$ et $b \in y$, alors $\mathfrak{M} \models a \leqslant b$ ou $\mathfrak{M} \models b \leqslant a$, puisque l'ordre $\leqslant$ est total dans $\mathfrak{M}$; on a donc xRy ou yRx.

Les éléments standards sont tous équivalents, et la classe qu'ils forment est inférieure à toutes les autres. En revanche, si a est un élément non standard, a et $a + a$ ne sont pas équivalents, et la classe de $a + a$ est strictement supérieure à celle de a.

Pour montrer que R est un ordre dense sur E, on montre d'abord que :

$$\mathscr{P} \vdash \forall v_0 \exists v_1 (v_1 \pm v_1 \simeq v_0 \vee v_1 \pm v_1 \simeq v_0 + \underline{1}) ,$$

ce qui se fait sans difficulté par induction sur v_0.

Si a et b sont des éléments de $\mathfrak{M}$, si on suppose par exemple que $a \leqslant b$, et si c est l'élément tel que $c + c = a + b$ ou $c + c = a + b + 1$, alors on voit facilement que $c \approx a$ si et seulement si $c \approx b$. Il en résulte que, s'il est faux que $a \approx b$, alors, strictement comprise entre la classe de a et celle de b, il y a la classe de c.

3. On démontre par récurrence sur n que, si $(b_0,b_1,...,b_n)$ est une suite d'entiers premiers entre eux deux à deux et si $(\alpha_0,\alpha_1,...,\alpha_n)$ est une autre suite de même longueur, alors il existe $a \in \mathbb{N}$ tel que, pour tout i compris entre 0 et n, on ait :

a congru à α_i modulo b_i.

Pour $n = 0$, il suffit de prendre $a = \alpha_0$. Voyons encore le cas $n = 1$. Puisque b_0 et b_1 sont premiers entre eux, le théorème de Bezout nous dit qu'il existe des éléments γ_0 et γ_1 dans $\mathbb{Z}$ tels que :

$$\gamma_0 b_0 + \gamma_1 b_1 = 1,$$

ce qui, en multipliant par $\alpha_1 - \alpha_0$, donne

$$(\alpha_1 - \alpha_0)\gamma_0 b_0 + \alpha_0 = (\alpha_0 - \alpha_1)\gamma_1 b_1 + \alpha_1,$$

et on obtient un élément m de $\mathbb{Z}$, à savoir $(\alpha_1 - \alpha_0)\gamma_0 b_0 + \alpha_0$, congru à α_0 modulo b_0 et à α_1 modulo b_1. Pour avoir un élément dans $\mathbb{N}$ possédant le même propriété, il suffit de lui ajouter kb_0b_1 pour un entier k assez grand.

Voyons maintenant le cas $n + 1$. Par hypothèse de récurrence, il existe un entier c tel que, pour tout i compris entre 0 et n, on ait :

c congru à α_i modulo b_i.

Mais b_{n+1} et $b_0b_1...b_n$ sont aussi premiers entre eux. On vient donc de voir qu'il existe $a \in \mathbb{N}$ tel que a soit congru à c modulo $b_0b_1...b_n$ et à α_{n+1} modulo b_{n+1}. Cela implique bien que, pour tout i compris entre 0 et $n + 1$,

a est congru à α_i modulo b_i.

4. Supposons que la formule $F[v_0,v_1,...,v_p]$ représente une fonction totale f de $\mathbb{N}^p$ dans $\mathbb{N}$. Alors (voir 4.4) :

$x = f(n_1,n_2,...,n_p)$ si et seulement si il existe y tel que $(\# F[x,n_1,n_2,...,n_p],y) \in Dem_0$.

Considérons alors la fonction g :

$$g(n_1,n_2,...,n_p) = \mu y((\# F[\beta_2^1(y),n_1,n_2,...,n_p],\beta_2^2(y)) \in Dem_0).$$

Elle est totale, récursive, et $f(n_1,n_2,...,n_p) = \beta_2^1(g(n_1,n_2,...,n_p))$.

5. Il s'agit d'une technique connue sous le nom de méthode du pléonasme : on énumère $T = \{ F_n \ ; \ n \in \mathbb{N} \}$ de telle sorte que la fonction $\lambda n.\# F_n$ soit une fonction récursive totale (voir 4.5 au chapitre 5). Pour chaque $n \in \mathbb{N}$, on appelle G_n la formule $F_1 \wedge F_2 \wedge ... \wedge F_n$. Posons $T' = \{ G_n \ ; \ n \in \mathbb{N} \}$. Alors il est clair que T et T' sont des

théories équivalentes et que la fonction $\lambda n.\# G_n$ est récursive totale et strictement croissante, ce qui implique que T' est une théorie récursive (exercice 12 du chapitre 5).

6. Il faut d'abord se persuader que cette question a un sens, c'est-à-dire vérifier que le grand théorème de Fermat s'exprime par une formule de $\mathscr{L}_0$, ce qui n'est pas le cas a priori à cause des exponentielles x^t, etc. On commence donc par éliminer ces exponentielles en utilisant des formules qui les représentent. Soit donc $F[v_0,v_1,v_2]$ une formule Σ telle que, pour tous entiers n, m et p, $\mathscr{P}_0 \vdash F[\underline{n},\underline{m},\underline{p}]$ si et seulement si $n = m^p$. On remarque alors que la négation du grand théorème de Fermat s'exprime dans le langage $\mathscr{L}_0$ par la formule close Σ suivante :

$$G = \exists v_0 \exists v_1 \exists v_2 \exists v_3 \exists v_4 \exists v_5 \exists v_6 (v_2 \geqslant 1 \wedge v_4 \geqslant 1 \wedge v_6 \geqslant 1 \wedge v_0 \geqslant 3 \wedge F[v_1,v_2,v_0] \wedge F[v_3,v_4,v_0] \wedge F[v_5,v_6,v_0] \wedge v_1 + v_3 = v_5).$$

Si G est vraie dans $\mathbb{N}$, alors elle est démontrable dans $\mathscr{P}_0$ (proposition 4.6), et le grand théorème de Fermat est réfutable dans $\mathscr{P}_0$.

7. a) Il est bien clair que si $\mathbb{N} \models \exists v_1 \mathfrak{Dem}[\underline{\# F},v_1]$, alors il existe un entier n tel que $\mathbb{N} \models \mathfrak{Dem}[\#F,n]$, et donc tel que $(\#F,n) \in$ Dem. Il en résulte que la formule F est vraiment démontrable dans $\mathscr{P}$, et donc qu'elle est vraie dans $\mathbb{N}$.

b) La preuve du second théorème d'incomplétude fournit un modèle $\mathfrak{M}$ de $\mathscr{P}$ et une formule close F tels que $\mathfrak{M} \models \exists v_1 \mathfrak{Dem}[\underline{\# F},v_1] \wedge \exists v_2 \mathfrak{Dem}[\underline{\# \neg F},v_2]$. Ceci montre que b) ne peut pas être vérifiée en même temps pour F et pour $\neg$F.

c) On suppose que c) est vrai pour toute formule close F et on en déduit une contradiction. Puisque, dans $\mathbb{N}$, F est vraie ou $\neg$F est vraie, $\mathscr{P}$ démontre F ou démontre $\neg$F, autrement dit $\mathscr{P}$ est une théorie complète : on sait que cela est faux.

d) Evidemment faux car d) implique c).

8. On peut prendre pour formule $F[v_0]$ la formule $\mathfrak{Dem}[\underline{\# 0 \simeq 1},v_0]$, et pour H la formule $G[v_0,v_1,\ldots,v_n] \Leftrightarrow \mathfrak{Dem}[\underline{\# 0 \simeq 1},v_0]$.

9. Supposons que : $\mathscr{P} \vdash \exists v_0 \mathfrak{Dem}[\underline{\# F},v_0] \Rightarrow F$; alors, par contraposition :

$$\mathscr{P} \vdash \neg F \Rightarrow \neg \exists v_0 \mathfrak{Dem}[\underline{\# F},v_0] ;$$

soit encore :

$$\mathscr{P} \cup \{ \neg F \} \vdash \neg \exists v_0 \mathfrak{Dem}[\underline{\# F},v_0].$$

Or $\neg \exists v_0 \mathfrak{Dem}[\# F,v_0]$ veut dire que F n'est pas démontrable dans $\mathscr{P}$, autrement dit que $\mathscr{P} \cup \{\neg F\}$ est une théorie cohérente. On a donc :

$$\mathscr{P} \cup \{ \neg F \} \vdash \mathrm{Coh}(\mathscr{P} \cup \{ \neg F \}),$$

ce qui implique, d'après le second théorème d'incomplétude de Gödel, que $\mathscr{P} \cup \{ \neg F \}$ n'est pas une théorie cohérente, donc que $\mathscr{P} \vdash F$.

10. a) On va montrer par induction sur la hauteur de la formule $G[v_1,v_2,\ldots,v_p]$ que, pour tous éléments $a_1,a_2,\ldots,a_p$ de N, on a :

$$\mathfrak{M} \models G[a_1,a_2,\ldots,a_p] \text{ si et seulement si } \mathfrak{N} \models G[a_1,a_2,\ldots,a_p].$$

C'est vrai si G est une formule atomique parce que $\mathfrak{N}$ est une sous-structure de $\mathfrak{M}$. Les connecteurs propositionnels n'offrent guère de difficulté. Voyons à titre d'exemple le cas de $\wedge$; on suppose donc que $G[v_1,v_2,\ldots,v_p] = G_1 \wedge G_2$ et que $a_1,a_2,\ldots,a_p$ sont des points de N. Alors :

$$\mathfrak{M} \models G[a_1,a_2,\ldots,a_p] \text{ si et seulement si } \mathfrak{M} \models G_1[a_1,a_2,\ldots,a_p] \text{ et } \mathfrak{M} \models G_2[a_1,a_2,\ldots,a_p].$$

Or par hypothèse d'induction :

$$\mathfrak{M} \models G_1[a_1,a_2,\ldots,a_p] \text{ si et seulement si } \mathfrak{N} \models G_1[a_1,a_2,\ldots,a_p],$$

et

$$\mathfrak{M} \models G_2[a_1,a_2,\ldots,a_p] \text{ si et seulement si } \mathfrak{N} \models G_2[a_1,a_2,\ldots,a_p] \text{ ;}$$

cela montre bien que :

$$\mathfrak{M} \models G[a_1,a_2,\ldots,a_p] \text{ si et seulement si } \mathfrak{N} \models G[a_1,a_2,\ldots,a_p].$$

Occupons-nous maintenant du quantificateur existentiel. On va supposer que $G[v_1,v_2,\ldots,v_p] = \exists v_0 F[v_0,v_1,\ldots,v_p]$, et soient $a_1,a_2,\ldots,a_p$ des points de N. Si on suppose que $\mathfrak{N} \models G[a_1,a_2,\ldots,a_p]$ alors il existe un point a_0 de N tel que $\mathfrak{N} \models F[a_0,a_1,\ldots,a_p]$ et par hypothèse d'induction $\mathfrak{M} \models F[a_0,a_1,\ldots,a_p]$ et donc $\mathfrak{M} \models G[a_1,a_2,\ldots,a_p]$.

Réciproquement, supposons que les points $a_1,a_2,\ldots,a_p$ sont dans N et qu'il existe a_0 dans M tel que $\mathfrak{M} \models F[a_0,a_1,\ldots,a_p]$. Considérons la formule :

$$H[v_0,v_1,\ldots,v_p] = (\neg\exists v_{p+1}F[v_{p+1},v_1,\ldots,v_p] \Rightarrow v_0 \simeq \underline{0}) \wedge$$
$$(\exists v_{p+1}F[v_{p+1},v_1,\ldots,v_p] \Rightarrow (F[v_0,v_1,\ldots,v_p] \wedge \forall v_{p+1} < v_0\, \neg F[v_{p+1},v_1,\ldots,v_p])) .$$

La formule H définit donc la fonction f de M^p dans M suivante :

- s'il existe au moins un élément $x \in M$ tel que $\mathfrak{M} \models F[x,a_1,a_2,\ldots,a_p]$, alors $f(a_1,a_2,\ldots,a_p)$ est le plus petit des éléments satisfaisant cette formule (qui existe à cause du schéma d'induction).
- sinon, $f(a_1,a_2,\ldots,a_p) = \mathbf{0}$.

Par hypothèse (parce que $\mathfrak{N}$ est clos pour les fonctions définissables) $f(a_1,a_2,\ldots,a_p)$ appartient à N. De la définition de H, il découle que $\mathfrak{M} \models F[f(a_1,a_2,\ldots,a_p),a_1,a_2,\ldots,a_p]$ et par hypothèse d'induction $\mathfrak{N} \models F[f(a_1,a_2,\ldots,a_p),a_1,a_2,\ldots,a_p]$ et donc $\mathfrak{N} \models G[a_1,a_2,\ldots,a_p]$.

b) Si X_1 et X_2 sont des sous-ensembles de M définissables respectivement par les formules $F_1[v_0]$ et $F_2[v_0]$, alors $X_1 \cap X_2$ est définissable par la formule $F_1 \wedge F_2$. On a des faits analogues pour la réunion et le complémentaire, ce qui montre bien que les sous-ensembles définissables de M forment une sous-algèbre de Boole de l'ensemble des parties de M.

Si f et g sont des fonctions définissables respectivement par $G_1[v_0,v_1]$ et $G_2[v_0,v_1]$, alors :

$$\{\, a \in M \,;\, f(a) = g(a) \,\} = \{\, a \in M \,;\, \mathfrak{M} \models \exists v_0(G_1[v_0,a] \wedge G_2[v_0,a]) \,\}.$$

qui est bien un ensemble définissable.

c) Supposons encore que f et g sont des fonctions définissables respectivement par $G_1[v_0,v_1]$ et $G_2[v_0,v_1]$; prenons par exemple $f + g$; elle est définissable par la formule :

$$\exists v_2 \exists v_3 (v_0 \simeq v_2 + v_3 \wedge G_1[v_2,v_1] \wedge G_2[v_3,v_1]).$$

On conclut tout aussi aisément pour $f \times g$ et Sf.

d) Soient f, g et h dans $\mathcal{F}$. Alors :

$$\{ a \in M ; f(a) = g(a) \} \cap \{ a \in M ; g(a) = h(a) \} \subseteq \{ a \in M ; f(a) = h(a) \},$$

ce qui montre que, si les deux premiers ensembles appartiennent à $\mathcal{U}$, le troisième appartient aussi à $\mathcal{U}$: la relation $\approx$ est donc transitive ; la symétrie et la réflexivité sont évidentes. De même :

$$\{ a \in M ; f(a) = f'(a) \} \cap \{ a \in M ; g(a) = g'(a) \} \subseteq \{ a \in M ; (f + g)(a) = (f' + g')(a) \},$$

et donc, si $f \approx f'$ et $g \approx g'$, alors $f + g \approx f' + g'$. On peut faire le même raisonnement pour le successeur et le produit.

e) Il s'agit simplement de vérifier que, si a et b sont des éléments de M, alors :

$$\bar{a} + \bar{b} = \overline{a + b},\ \bar{a} \times \bar{b} = \overline{a \times b} \text{ et } S\bar{a} = \overline{Sa},$$

ce qui est évident.

f) On raisonne par induction sur la complexité de F. On va, à titre d'exemple traiter le cas de $\neg$ et de $\exists$.

• $\neg$: on suppose que $F[v_1,v_2,\ldots,v_p] = \neg G[v_1,v_2,\ldots,v_p]$, et que, pour tous $f_1,f_2,\ldots f_p$ de $\mathcal{F}$,

$\mathcal{F}/\mathcal{U} \models G[f_1/\mathcal{U},f_2/\mathcal{U},\ldots,f_p/\mathcal{U}]$ si et seulement si $\{ a \in M ; \mathfrak{M} \models G[f_1(a),f_2(a),\ldots,f_p(a)] \} \in \mathcal{U}$.

Mais on voit que :

$$\mathcal{F}/\mathcal{U} \models G[f_1/\mathcal{U},f_2/\mathcal{U},\ldots,f_p/\mathcal{U}] \text{ si et seulement si } \mathcal{F}/\mathcal{U} \not\models F[f_1/\mathcal{U},f_2/\mathcal{U},\ldots,f_p/\mathcal{U}],$$

et, parce que $\mathcal{U}$ est un ultrafiltre :

$$\{ a \in M ; \mathfrak{M} \models G[f_1(a),f_2(a),\ldots,f_p(a)] \} \in \mathcal{U}$$

si et seulement si $\{ a \in M ; \mathfrak{M} \models F[f_1(a),f_2(a),\ldots,f_p(a)] \} \notin \mathcal{U}$.

• $\exists$: on suppose maintenant que $F[v_1,v_2,\ldots,v_p] = \exists v_0 G[v_0,v_1,\ldots,v_p]$ et que G satisfait l'hypothèse d'induction. Supposons d'abord que :

$$\mathcal{F}/\mathcal{U} \models F[f_1/\mathcal{U},f_2/\mathcal{U},\ldots,f_p/\mathcal{U}].$$

Il existe donc une fonction $f_0 \in \mathcal{F}$ telle que $\mathcal{F}/\mathcal{U} \models G[f_0/\mathcal{U},f_1/\mathcal{U},\ldots,f_p/\mathcal{U}]$, et, par hypothèse d'induction $\{ a \in M ; \mathfrak{M} \models G[f_0(a),f_1(a),\ldots,f_p(a)] \} \in \mathcal{U}$, d'où il découle que $\{ a \in M ; \mathfrak{M} \models F[f_1(a),f_2(a),\ldots,f_p(a)] \} \in \mathcal{U}$.

Réciproquement, supposons que $A = \{ a \in M ; \mathfrak{M} \models F[f_1(a),f_2(a),\ldots,f_p(a)] \} \in \mathcal{U}$. Considérons encore (voir a)) la formule $H[v_0,v_1,\ldots,v_p]$:

$$(\exists v_{p+1} G[v_{p+1},v_1,v_2,\ldots,v_p] \Longrightarrow (G[v_0,v_1,\ldots,v_p) \wedge \forall v_{p+2} < v_0 \neg G[v_{p+2},v_1,v_2,\ldots,v_p])) \wedge$$
$$(\neg \exists v_{p+1} G[v_{p+1},v_1,v_2,\ldots,v_p] \Longrightarrow v_0 \simeq \underline{0}).$$

La formule H définit une fonction f_0, et pour tout $a \in A$, on a :

$$\mathfrak{M} \models G[f_0(a),f_1(a),\ldots,f_p(a)],$$

et donc, par hypothèse d'induction,

$$\mathcal{I}/\mathcal{U} \models G[f_0/\mathcal{U}, f_1/\mathcal{U}, \ldots, f_p/\mathcal{U}] \text{ et } \mathcal{I}/\mathcal{U} \models F[f_1/\mathcal{U}, f_2/\mathcal{U}, \ldots, f_p/\mathcal{U}].$$

Soient maintenant $d_1, d_2, \ldots, d_p$ des points de M et $\overline{d}_1$, $\overline{d}_2, \ldots, \overline{d}_p$ les fonctions constantes correspondantes. Alors $\{ a \in M : \mathfrak{M} \models F[\overline{d}_1(a), \overline{d}_2(a), \ldots, \overline{d}_p(a)] \}$ est égal à M tout entier si $\mathfrak{M} \models F[d_1, d_2, \ldots, d_p]$ et est vide sinon. Donc :

$$\{ a \in M : \mathfrak{M} \models F[\overline{d}_1(a), \overline{d}_2(a), \ldots, \overline{d}_p(a)] \} \in \mathcal{U} \quad \text{si et seulement si} \quad \mathfrak{M} \models F[d_1, d_2, \ldots, d_p],$$

ce qui veut exactement dire que l'application de $\mathfrak{M}$ dans $\mathcal{I}/\mathcal{U}$ qui à a associe $\overline{a}$ est élémentaire.

g) Soit $F[v_0, v_1, w_0, w_1, \ldots, w_p]$ une formule de $\mathcal{L}_0$. Notons :

$$\text{Fonc}_F[w_0, w_1, \ldots, w_p] = \forall v_0 \exists! v_1 \, F[v_0, v_1, w_0, w_1, \ldots, w_p],$$

qui est la formule qui exprime que F, lorsqu'on a substitué des paramètres aux variables w_i, définit une fonction. On doit montrer que :

$$\mathfrak{M} \models \forall w_0 \forall w_1 \ldots \forall w_p (\text{Fonc}_F[w_0, w_1, \ldots, w_p] \Longrightarrow \forall v_2 \exists v_3 \forall v_0 \forall v_1 ((v_0 < v_2 \land F[v_0, v_1, w_0, w_1, \ldots, w_p]) \Longrightarrow v_1 < v_3)).$$

Puisque $\mathfrak{M}$ est une extension élémentaire de $\mathbb{N}$, il suffit de voir que cette même formule est vraie dans $\mathbb{N}$. Or, si pour des entiers m_0, m_1, ..., m_p, la formule $F[v_0, v_1, m_0, m_1, \ldots, m_p]$ définit, sur $\mathbb{N}$, une fonction, disons f, et si n_2 est un entier, il existe bien un entier n_3, à savoir $\sup\{ f(x) + 1 \,;\, x < n_2 \}$ tel que :

$$\mathbb{N} \models \forall v_0 \forall v_1 ((v_0 < n_2 \land F[v_0, v_1, m_0, m_1, \ldots, m_p]) \Longrightarrow v_1 < n_3).$$

h) On appelle encore $\mathcal{B}$ l'algèbre de Boole des sous-ensembles de M définissables à paramètres dans M, et on considère le sous-ensemble suivant de $\mathcal{B}$:

$$\{ [a,b] \,;\, a \in \mathbb{N}, b \in M - \mathbb{N} \}$$

(où $[a,b]$ désigne l'ensemble des points de M compris entre a et b). Cet ensemble est clos par intersection finie et ne contient pas l'ensemble vide. On en déduit qu'il existe un ultrafiltre $\mathcal{U}$ de $\mathcal{B}$ qui le contient. Appelons $\mathfrak{N}$ la structure $\mathcal{I}/\mathcal{U}$ construite ci-dessus, considérée comme extension élémentaire de $\mathfrak{M}$. On va montrer qu'elle satisfait la propriété désirée.

Soit $f/\mathcal{U} \in \mathfrak{N}$. Prenons un élément quelconque c non standard de $\mathfrak{M}$. On sait, d'après la question précédente, qu'il existe $d \in M$, tel que si $x \in M$ et $x < c$, alors $f(x) < d$. Appelons $\overline{d}$ la fonction constante égale à d et rappelons que l'on a identifié $\overline{d}/\mathcal{U} \in \mathfrak{N}$ et d. Alors :

$$[0,c] \subseteq \{ a \in M \,;\, f(a) < \overline{d}(a) \},$$

et, comme $[0,c] \in \mathcal{U}$, on a bien, d'après f), $f/\mathcal{U} < d$.

11. a) Appelons H la conjonction des sept axiomes de $\mathcal{P}_0$, et soit T une théorie vérifiée par $\mathbb{N}$. Si T était décidable, alors l'ensemble $\{ \# F \,;\, \#(H \Longrightarrow F) \in Th(T) \}$ serait récursif ; or cet ensemble est exactement $Th(T \cup \mathcal{P}_0)$ qui est une théorie cohérente ($\mathbb{N}$ en est un modèle) contenant $\mathcal{P}_0$, ce qui contredit le premier théorème de Gödel.

b) On va montrer comment construire la formule F^* à partir de F. Le procédé que l'on va décrire est effectif, et il n'y a aucune difficulté à montrer l'existence d'une fonction récursive primitive α qui, au numéro de Gödel de F, fait correspondre celui de F^*.

Cette construction se fait par induction sur la hauteur de F. Il faut commencer par les formules atomiques, qui dans $\mathscr{L}_0$, sont de la forme $t \simeq s$ (t et s termes de $\mathscr{L}_0$). On se débarrasse d'abord du cas où t et s sont des termes simples, c'est-à-dire où F est de l'une des formes suivantes :

- $F = v_i \simeq \underline{0}$, alors $F^* = G_1[v_i]$;
- $F = v_i \simeq v_j$, alors $F^* = G_0[v_i] \wedge G_0[v_j] \wedge v_i \simeq v_j$;
- $F = v_i \simeq \underline{S}v_j$, alors $F^* = G_0[v_i] \wedge G_0[v_j] \wedge G_2[v_i,v_j]$;
- $F = v_i \simeq v_j \underline{+} v_k$, alors $F^* = G_0[v_i] \wedge G_0[v_j] \wedge G_0[v_k] \wedge G_3[v_i,v_j,v_k]$;
- $F = v_i \simeq v_j \underline{\times} v_k$, alors $F^* = G_0[v_i] \wedge G_0[v_j] \wedge G_0[v_k] \wedge G_4[v_i,v_j,v_k]$.

On s'occupe ensuite des formules de la forme $v_i = t$ où t est un terme. Cela se fait par induction sur t. A titre d'exemple, traitons le cas où $F = v_i \simeq t_1 \underline{+} t_2$, en supposant que l'on ait déjà construit les formules $(v_i \simeq t_1)^*$ et $(v_i \simeq t_2)^*$. On choisit des variables w_0 et w_1 qui n'apparaissent pas dans v_i, t_1, t_2. On pose :

$$F^* = \exists w_0 \exists w_1((w_0 \simeq t_1)^* \wedge (w_1 \simeq t_2)^* \wedge (v_i \simeq w_0 \underline{+} w_1)^*).$$

On termine les formules atomiques en posant $(t_1 \simeq t_2)^* = \exists w_0((w_0 \simeq t_1)^* \wedge (w_0 \simeq t_2)^*)$, où, encore une fois, w_0 est une variable n'apparaissant ni dans t_1 ni dans t_2.

Ensuite, on fait une induction sans problème sur la hauteur de F :

- $(\neg F)^* = \neg F^*$;
- $(F_1 \wedge F_2)^* = F_1^* \wedge F_2^*$;
- $(F_1 \vee F_2)^* = F_1^* \vee F_2^*$;
- $(F_1 \Longrightarrow F_2)^* = F_1^* \Longrightarrow F_2^*$;
- $(F_1 \Longleftrightarrow F_2)^* = F_1^* \Longleftrightarrow F_2^*$;
- $(\exists w F[w])^* = \exists w_0(G_0[w_0] \wedge F[w_0]^*)$ où w_0 est une variable qui n'apparaît ni dans G_0 ni dans F ;
- $(\forall w F[w])^* = \forall w_0(G_0[w_0] \Longrightarrow F[w_0]^*)$ où w_0 est une variable qui n'apparaît ni dans G_0 ni dans F.

c) Il est évident que 1) implique 2), et que 3) implique 1). Il reste donc à voir que 2) implique 3). On va utiliser le théorème de complétude et montrer, sous la condition $T^- \vdash G$, que $T \cup \{ \neg G^* \}$ n'a pas de modèle : supposons le contraire et soit $\mathfrak{N}$ la $\mathscr{L}_0$-structure définissable dans un modèle $\mathfrak{M}$ de $T \cup \{ \neg G^* \}$. Puisque $\mathfrak{M}$ est un modèle de T, $\mathfrak{N}$ est (d'après b)) un modèle de T^-, donc de G ; puisque $\mathfrak{M}$ est un modèle de $\neg G^*$, $\mathfrak{N}$ est un modèle de $\neg G$, ce qui est impossible.

d) On va d'abord montrer que toute théorie cohérente dans $\mathscr{L}$ contenant $T_0 \cup \{ H^* \}$ est indécidable (rappelons que H est la conjonction des axiomes de $\mathscr{P}_0$). En effet, soit T une telle théorie, et, comme précédemment, considérons :

$$T^- = \{ F \ ; F \text{ est une formule close de } \mathscr{L}_0 \text{ et } T \vdash F^* \}.$$

C'est une théorie cohérente contenant $\mathscr{P}_0$, donc indécidable. Or, si T était décidable, T^- le serait aussi car $T^- \vdash F$ si et seulement si $T \vdash F^*$ (et le passage de F à F^* est effectif).

Supposons maintenant que $\mathbb{N}$ soit définissable dans $\mathfrak{M}$ et soit T une théorie dans $\mathscr{L}$ dont $\mathfrak{M}$ est modèle. Il s'agit de montrer que T est indécidable. Soit K la conjonction des formules de $T_0 \cup \{H^*\}$ (c'est une théorie finie). Alors, on voit que $\mathfrak{M}$ est un modèle de $T' = T \cup \{K\}$, qui est donc cohérente, et d'après ce que nous avons vu, non décidable. Or, pour toute formule F de $\mathscr{L}$,

$$T' \vdash F \quad \text{si et seulement si} \quad T \vdash K \Rightarrow F,$$

ce qui montre que T non plus n'est pas décidable.

e) Il n'est pas difficile de définir $\mathbb{N}$ dans $\mathbb{Z}$; par exemple avec les formules suivantes :

- $G_0(v_0) = \exists v_1 \exists v_2 \exists v_3 \exists v_4 (v_0 \simeq ((v_1 \underline{\times} v_1) \underline{+} (v_2 \underline{\times} v_2) \underline{+} (v_3 \underline{\times} v_3) \underline{+} (v_4 \underline{\times} v_4)))$;

(c'est ici que l'on se sert du théorème de Lagrange)

- $G_1[v_0] = v_0 \simeq \underline{0}$;
- $G_2[v_0,v_1] = G_0[v_0] \wedge G_0[v_1] \wedge \exists v_2 \forall v_3 (v_2 \underline{\times} v_3 \simeq v_3 \wedge v_0 \simeq v_1 \underline{+} v_2)$;
- $G_3[v_0,v_1,v_2] = G_0[v_0] \wedge G_0[v_1] \wedge G_0[v_2] \wedge v_0 \simeq v_1 \underline{+} v_2$;
- $G_4[v_0,v_1,v_2] = G_0[v_0] \wedge G_0[v_1] \wedge G_0[v_2] \wedge v_0 \simeq v_1 \underline{\times} v_2$.

On en déduit que $\mathbb{Z}$ est fortement indécidable et que toute théorie dans $\mathscr{L}$ dont $\mathbb{Z}$ est modèle est indécidable ; par exemple, la théorie des anneaux, celle des anneaux commutatifs, etc.

f) On s'aperçoit tout d'abord que, si x est un élément de M qui appartient à $\mathbb{N} \times \mathbb{N}$, disons $x = (n,m)$, il y a exactement deux éléments y de M, à savoir m et $(n + m, n \cdot m)$ tels que $(x,y) \in R^{\mathfrak{M}}$, tandis que, si $x \in \mathbb{N}$, l'ensemble des éléments y de M tels que $(x,y) \in R^{\mathfrak{M}}$ est infini ; cela permet de définir $\mathbb{N}$ dans $\mathfrak{M}$ par la formule :

$$G_0[v_0] = \exists v_1 \exists v_2 \exists v_3 (Rv_0v_1 \wedge Rv_0v_2 \wedge Rv_0v_3 \wedge \neg v_1 \simeq v_2 \wedge \neg v_2 \simeq v_3 \wedge \neg v_3 \simeq v_1).$$

L'addition et la multiplication sont alors faciles à définir :

$G_3[v_0,v_1,v_2] = G_0[v_0] \wedge G_0[v_1] \wedge G_0[v_2] \wedge \exists v_3 \exists v_4 (Rv_1v_3 \wedge Rv_3v_2 \wedge Rv_3v_4 \wedge Rv_0v_4)$;

$G_4[v_0,v_1,v_2] = G_0[v_0] \wedge G_0[v_1] \wedge G_0[v_2] \wedge \exists v_3 \exists v_4 (Rv_1v_3 \wedge Rv_3v_2 \wedge Rv_3v_4 \wedge Rv_4v_0)$.

Ensuite, le zéro et le un se définissent comme les éléments neutres de l'addition et de la multiplication respectivement, et la fonction successeur se définit à l'aide de l'addition.

On en déduit que $\mathfrak{M}$ est fortement indécidable et que la théorie vide dans le langage ne comportant qu'un seul symbole de prédicat binaire est indécidable.

g) Puisqu'on dispose de l'addition, on peut définir l'ordre sur les entiers, le zéro, l'élément 1 et la fonction successeur. Il suffit de montrer que la multiplication est définissable dans $\mathfrak{M}$. On commence par définir le ppcm de deux entiers par la formule :

$$G_5[v_0,v_1,v_2] = Dv_1v_0 \wedge Dv_2v_0 \wedge \forall v_3((Dv_1v_3 \wedge Dv_2v_3) \Rightarrow Dv_0v_3).$$

Or le ppcm de y et de y+1 est toujours $y\cdot(y+1)$, ce qui fait que la relation $x = y\cdot(y+1)$ est définie par la formule :

$$G_6[v_0,v_1] = G_5[v_0,v_1,v_1 \pm \underline{1}].$$

On remarque que, pour tous x et y dans $\mathbb{N}$, on a :

$$(x+y)\cdot(x+y+1) = x\cdot(x+1) + y\cdot(y+1) + 2xy,$$

et on peut donc poser :

$$\psi_4[v_0,v_1,v_2] = \exists v_3 \exists v_4 \exists v_5 \exists v_6 (v_3 \simeq v_0 \pm v_0 \wedge G_6[v_4,v_1 \pm v_2] \wedge G_6[v_5,v_1] \wedge G_6[v_6,v_2] \wedge v_4 \simeq (v_5 \pm v_6) \pm v_3).$$

12. a) A l'aide d'une récurrence sans problème sur la hauteur de F : cela revient à montrer que la classe des ensembles récursivement énumérables est close par conjonction, disjonction, quantification existentielle et quantification universelle bornée.

b) Soit f une fonction récursive de $\mathbb{N}$ dans $\mathbb{N}$; d'après le théorème de représentation bis (4.6), il existe une formule sigma $F[v_0,v_1]$ représentant f. Réciproquement, si :

$$\text{Graph}(f) = \{ (n,f(n)) \; ; \; n \in \mathbb{N} \} = \{ (n,m) \; ; \; \mathbb{N} \models F[m,n] \} = \{ (n,m) \; ; \; \mathscr{P}_0 \vdash F[\underline{m},\underline{n}] \},$$

où F est une formule Σ, alors , par a), Graph(f) est récursivement énumérable. Or f est une fonction totale, donc :

$(n,m) \notin \text{Graph}(f)$ si et seulement si il existe $m' \neq m$ tel que $(n,m') \in \text{Graph}(f)$,

ce qui fait que le complémentaire de Graph(f) est aussi récursivement énumérable, et que Graph(f) est récursif (chapitre 5, 4.2). Ainsi, f est récursive (chapitre 5, exercice 10).

c) Si $F[v_0,v_1]$ est une formule Σ, alors pour tous entiers n et m,

$\mathbb{N} \models F[m,n]$ si et seulement si il existe une démonstration de $F[\underline{m},\underline{n}]$ dans $\mathscr{P}_0$ (proposition 4.6) ; a fortiori

$\mathbb{N} \models F[m,n]$ si et seulement si il existe une démonstration de $F[\underline{m},\underline{n}]$ dans $\mathscr{P}$.

Soit α la fonction à trois variables définie de la façon suivante :

- Si a est le numéro de Gödel d'une formule Σ à deux variables libres, disons $F[v_0,v_1]$, alors $\alpha(a,m,n) = \# F[\underline{m},\underline{n}]$;
- Sinon, $\alpha(a,m,n) = 0$.

Cette fonction α est récursive primitive et, si a est le numéro de Gödel de la formule F, alors, pour tous entiers n et m, on a :

$\mathbb{N} \models F[m,n]$ si et seulement si il existe $b \in \mathbb{N}$ tel que $(\alpha(a,m,n),b) \in \text{Dem}$.

On peut alors définir la fonction partielle k :

$$k(a,n) = \mu y \; (\alpha(a,\beta_2^1(y),n),\beta_2^2(y)) \in \text{Dem},$$

et poser :

$$h(a,n) = \beta_2^1(k(a,n)).$$

d) Le fait que g soit récursive n'est pas difficile à voir : elle est définie par cas et les relations : a est le numéro de Gödel d'une formule Σ, ou b est le numéro de Gödel d'une démonstration dans $\mathscr{P}$ de la formule, etc. sont récursives. Montrons qu'elle est totale : soient a, b et n des entiers, et on suppose que a est le numéro de Gödel d'une formule Σ, disons $F[v_0,v_1]$ et que b est le numéro de Gödel d'une démonstration dans $\mathscr{P}$

de $\forall v_1 \exists v_0 F[v_0,v_1]$. Il s'agit de se rendre compte qu'il existe $m \in \mathbb{N}$ telle que $\mathscr{P} \vdash F[\underline{m},\underline{n}]$. Mais, puisque $\mathbb{N}$ est un modèle de $\mathscr{P}$, on a :

$$\mathbb{N} \models \forall v_1 \exists v_0 F[v_0,v_1],$$

et donc, il existe un entier m tel que $\mathbb{N} \models F[\underline{m},\underline{n}]$; or $F[\underline{m},\underline{n}]$ est une formule Σ, d'où (proposition 4.6) :

$$\mathscr{P} \vdash F[\underline{m},\underline{n}].$$

e) L'ensemble de fonctions :

$$\mathscr{E} = \{ \lambda n.g(a,b,n) \text{ ; a et b dans } \mathbb{N} \}$$

est, d'après ce qui précède, exactement égal à l'ensemble de toutes les fonctions récursives prouvablement totales. On applique alors un argument diagonal : la fonction $\lambda n.g(\beta_2^1(n),\beta_2^2(n),n) + 1$ est récursive totale mais ne peut pas appartenir à $\mathscr{E}$.

13. a) Si $\{ F_1,F_2,...,F_n \}$ est un ensemble fini de formules closes, $\mathscr{P} \cup \{ F_1,F_2,...,F_n \}$ est une théorie récursive. Si elle est cohérente, elle ne peut pas être complète, d'après le premier théorème de Gödel (4.3).

b) On fait la construction par récurrence sur la longueur de s : en supposant que s appartienne à $\{0,1\}^n$, et en supposant que les formules $F_\emptyset$, $F_{(s(0))}$, $F_{(s(0),s(1))}$, ..., $F_{(s(0),s(1),\cdots,s(n-1))}$ aient déjà été construites de telle sorte que :

$$\mathscr{P} \cup \{ F_\emptyset ,F_{(s(0))} ,F_{(s(0),s(1))} ,F_{(s(0),s(1),\cdots,s(n-1))} \}$$

soit une théorie cohérente, on va construire les formules $F_{(s(0),s(1),\cdots,s(n-1),0)}$ et $F_{(s(0),s(1),\cdots,s(n-1),1)}$. Puisque $\mathscr{P} \cup \{ F_\emptyset ,F_{(s(0))} ,F_{(s(0),s(1))} ,F_{(s(0),s(1),\cdots,s(n-1))} \}$ n'est pas une théorie complète (on l'a vu en a)), il existe une formule G qui n'est ni démontrée, ni réfutée par cette théorie, et on pose :

$$F_{(s(0),s(1),\cdots,s(n-1),0)} = G \quad \text{et} \quad F_{(s(0),s(1),\cdots,s(n-1),1)} = \neg G.$$

c) Pour chaque σ dans $\{0,1\}^{\mathbb{N}}$, posons :

$$T_\sigma = \mathscr{P} \cup \{ F_\emptyset ,F_{(\sigma(0))} ,F_{(\sigma(0),\sigma(1))} ,\ldots, F_{(\sigma(0),\sigma(1),\cdots,\sigma(n-1))} \cdots \}.$$

Chaque sous-ensemble fini de T_σ est inclus dans un ensemble de la forme :

$$\mathscr{P} \cup \{ F_\emptyset ,F_{s(0)} ,F_{(s(0),s(1))} ,\cdots ,F_{(s(0),s(1),\cdots,s(n-1))} \},$$

avec $n \in \mathbb{N}$ et $s \in \{ 0,1 \}^n$, et est donc cohérent. Il en résulte, par le théorème de finitude, que T_σ est une théorie cohérente. Soient maintenant σ et τ deux éléments distincts de $\{0,1\}^{\mathbb{N}}$, et soit n le plus petit des entiers x tels que $\sigma(x) \neq \tau(x)$. Pour fixer les idées, supposons que $\sigma(n) = 0$ et $\tau(n) = 1$. Alors la formule $F_{(\tau(0),\tau(1),\cdots,\tau(n-1),\tau(n))}$ qui appartient à T_τ et qui est égale à $F_{(\sigma(0),\sigma(1),\cdots,\sigma(n-1),1)}$ est la négation de $F_{(\sigma(0),\sigma(1),\cdots,\sigma(n-1),0)}$ qui, elle, appartient à T_σ : T_σ et T_τ ne sont donc pas équivalentes.

On a ainsi trouvé $2^{\aleph_0}$ théories dans $\mathscr{L}_0$, autant que d'éléments dans $\{0,1\}^{\mathbb{N}}$, deux à deux non équivalentes, qui contiennent toutes $\mathscr{P}$.

14. a) Si $\mathfrak{M}$ est dénombrable, il n'y a qu'un nombre dénombrable de formules avec paramètres dans $\mathfrak{M}$, et donc pas plus de sous-ensembles de $\mathbb{N}$ définissables dans $\mathfrak{M}$.

b) Il existe une formule $F[v_0,v_1]$ de $\mathscr{L}_0$, telle que, pour tous entiers n et m,

$\mathbb{N} \models F[n,m]$ si et seulement si le $(n+1)$-ème nombre premier divise m.

Soit X un sous-ensemble de $\mathbb{N}$. Ajoutons au langage $\mathscr{L}_0$ un nouveau symbole de constante c, et considérons la théorie T_X suivante dans le langage ainsi obtenu :

$T_X = \{ G[\underline{n}_0,\underline{n}_1,\ldots,\underline{n}_p]$; p est un entier, $G[v_0,v_1,\ldots,v_p]$ est une formule de $\mathscr{L}_0$, n_0, $n_1,\ldots,n_p$ sont des entiers et $\mathbb{N} \models G[\underline{n}_0,\underline{n}_1,\ldots,\underline{n}_p] \} \cup \{ F[n,c] ; n \in X \} \cup \{ \neg F[n,c] ; n \notin X \}$.

Cette théorie est cohérente, d'après le théorème de finitude : on remarque que toute partie finie de T_X est incluse dans un ensemble de la forme :

$T_Y = \{ G(\underline{n}_0,\underline{n}_1,\ldots,\underline{n}_p)$; p est un entier, $G[v_0,v_1,\ldots,v_p]$ est une formule de $\mathscr{L}_0$, n_0, $n_1,\ldots,n_p$ sont des entiers et $\mathbb{N} \models G[\underline{n}_0,\underline{n}_1,\ldots,\underline{n}_p] \} \cup \{ F[n,c] ; n \in Y \} \cup \{ \neg F[n,c] ; n \notin Y \}$,

où Y est une partie finie de X. La structure $\mathbb{N}$ avec la constante c interprétée par :

$$\prod_{k \in Y} \pi(k),$$

où $\pi(k)$ est le $(k+1)$-ème nombre premier, est un modèle de T_Y. Il en résulte (chapitre 8, 1.5) que T_X a un modèle dénombrable, que l'on appellera $\mathfrak{M}$. On peut même considérer (chapitre 8, 2.3) que ce modèle est une extension élémentaire de $\mathbb{N}$. Par abus de langage, appelons c l'interprétation de c dans $\mathfrak{M}$. Alors :

$$X = \{ n \in \mathbb{N} ; \mathfrak{M} \models F[n,c] \},$$

ce qui montre que X est définissable dans $\mathfrak{M}$.

c) Pour chaque extension élémentaire dénombrable $\mathfrak{M}$ de $\mathbb{N}$, considérons :

$$S(\mathfrak{M}) = \{ X ; X \subseteq \mathbb{N} \text{ et } X \text{ est définissable dans } \mathfrak{M} \}.$$

On a vu en a) que $S(\mathfrak{M})$ est un sous-ensemble dénombrable de $\mathscr{P}(\mathbb{N})$, et en b) que :

$$\mathfrak{P}(\mathbb{N}) = \bigcup \{ S(\mathfrak{M}) ; \mathfrak{M} \succ \mathbb{N} \text{ et } \mathfrak{M} \text{ dénombrable} \}.$$

Si λ est la cardinalité de l'ensemble $\{ S(\mathfrak{M}) ; \mathfrak{M} \succ \mathbb{N}$ et $\mathfrak{M}$ dénombrable $\}$, alors $\lambda \times \aleph_0 = 2^{\aleph_0}$, d'où il suit que $\lambda = 2^{\aleph_0}$. Or, si $\mathfrak{M}$ et $\mathfrak{N}$ sont deux extensions élémentaires de $\mathbb{N}$ et si f est un isomorphisme de $\mathfrak{M}$ sur $\mathfrak{N}$, alors l'image par f d'un sous-ensemble de $\mathbb{N}$ définissable dans $\mathfrak{M}$ est définissable dans $\mathfrak{N}$ (au moyen de la même formule). Donc si $S(\mathfrak{M})$ est différent de $S(\mathfrak{N})$, alors $\mathfrak{M}$ et $\mathfrak{N}$ ne sont certainement pas isomorphes : il y a donc $2^{\aleph_0}$ extensions élémentaires dénombrables de $\mathbb{N}$ deux à deux non isomorphes.

15. a) Epiménides ne peut pas dire la vérité, car alors, étant crétois, il devrait mentir. Mais s'il ment, il est faux que les crétois sont menteurs, et donc il doit dire la vérité.

En fait, ce raisonnement n'est pas difficile à mettre en défaut ; d'abord parce qu'un menteur peut dire occasionnellement la vérité. Ensuite, il est possible qu'Epiménides mente, la vérité étant que certains crétois, dont lui-même, sont menteurs.

b) Ce barbier est une femme ; sinon, on ne pourrait pas répondre à la question : « ce barbier se rase-t-il lui-même ? » sans aboutir à une contradiction.

CHAPITRE 7

1. a) Pour cette question, on écrira ε au lieu de ε_φ. Vérifions les axiomes de ZF^-.

• Extensionnalité : soient x et y deux entiers tels que, pour tout entier z, on ait $z \,\varepsilon\, x$ si et seulement si $z \,\varepsilon\, y$, c'est-à-dire que $z \in \varphi(x)$ si et seulement si $z \in \varphi(y)$; on en déduit que $\varphi(x) = \varphi(y)$, et, parce que φ est bijective, que $x = y$.

• Paire : soient x et y deux entiers ; on cherche un entier z tel que l'ensemble (au sens intuitif) des entiers t tels que $t \,\varepsilon\, z$ (ou encore $t \in \varphi(z)$) soit la paire (au sens intuitif) $\{x,y\}$; on doit donc avoir $\varphi(z) = \{x,y\}$, ce qui définit un unique entier z, puisque φ est une bijection.

• Réunion : soit x un entier ; posons $z = \bigcup_{t \in \varphi(x)} \varphi(t)$ et $y = \varphi^{-1}(z)$; on voit que, pour tout entier u, $u \in \varphi(y)$ si et seulement si il existe un entier t tel que $t \in \varphi(x)$ et $u \in \varphi(t)$; exprimé avec la relation ε, cela signifie que, pour tout u, $u \,\varepsilon\, y$ si et seulement si il existe t tel que $t \,\varepsilon\, x$ et $u \,\varepsilon\, t$; on voit donc que y est, dans l'univers $\langle \mathbb{N}, \varepsilon \rangle$, la réunion des éléments de x.

• Parties : soit x un entier ; on cherche un entier y tel que, pour tout entier z, $z \in \varphi(y)$ si et seulement si quel que soit t appartenant à $\varphi(z)$, t appartient à $\varphi(x)$; autrement dit, pour tout z, $z \in \varphi(y)$ si et seulement si $\varphi(z) \in \mathfrak{P}(\varphi(x))$; on voit facilement que $\mathfrak{P}(\varphi(x))$ est un sous-ensemble fini de W (ensemble des parties finies de $\mathbb{N}$) ; son image réciproque par la bijection φ est donc une partie finie de $\mathbb{N}$, donc un élément de W, lequel admet un unique antécédent par φ ; l'ensemble cherché est donc : $y = \varphi^{-1}(\overline{\varphi}^{-1}(\mathfrak{P}(\varphi(x))))$.

• Remplacement : soient x un entier et $F[v_0,v_1]$ une formule du langage de la théorie des ensembles, fonctionnelle en v_0 (dans l'univers $\langle \mathbb{N}, \varepsilon \rangle$) (on prend ici une formule sans paramètres pour simplifier ; la présence de paramètres ne changerait pas grand chose à la démonstration qui va suivre) ; on cherche un entier y qui soit « l'image de x par F », c'est-à-dire tel que, pour tout entier z, $z \,\varepsilon\, y$ si et seulement si il existe t tel que $t \,\varepsilon\, x$ et $\langle \mathbb{N}, \varepsilon \rangle \models F[t,z]$; désignons par h la fonction partielle de $\mathbb{N}$ dans $\mathbb{N}$ définie comme suit : pour tous entiers n et m, $h(n) = m$ si et seulement si $\langle \mathbb{N}, \varepsilon \rangle \models F[n,m]$ (il s'agit d'une fonction partielle parce que F est fonctionnelle) ; on voit alors facilement qu'en posant $y = \varphi^{-1}(\overline{h}(\varphi(x)))$, on obtient l'ensemble cherché (on aura remarqué que l'ensemble $\overline{h}(\varphi(x))$, image directe par la fonction partielle h de l'ensemble fini $\varphi(x)$, est bien une partie finie de $\mathbb{N}$, et admet donc un (unique) antécédent par φ).

• Négation de l'axiome de l'infini : on raisonne par l'absurde et on suppose que $\langle \mathbb{N}, \varepsilon \rangle$ satisfait l'axiome de l'infini. Alors il existe des entiers a et f tels que :

$\langle \mathbb{N}, \varepsilon \rangle \models$ « f est une application injective non surjective de a dans lui même » ;

on voit facilement que l'ensemble :

$$\{ (x,y) \in \varphi(a)^2 \, ; \, \langle \mathbb{N}, \varepsilon \rangle \models « y = f(x) » \}$$

est une application injective non surjective de $\varphi(a)$ dans lui-même, ce qui est impossible puisque $\varphi(a)$ est un ensemble fini.

On suppose maintenant que, pour tous entiers x et y, $x \in \varphi(y)$ implique $x < y$. Cela implique en particulier que $\varphi(0)$ est l'ensemble vide.

• Axiome de fondation : on se donne un entier $x > 0$ (donc distinct de l'ensemble vide dans $<\mathbb{N},\varepsilon>$), et on cherche un entier y tel que (dans $<\mathbb{N},\varepsilon>$) $y \, \varepsilon \, x$ et $y \cap x = \emptyset$ (cette dernière condition signifiant que, pour tout t, si $t \, \varepsilon \, y$, alors on n'a pas $t \, \varepsilon \, x$) ; il suffit de prendre pour y le plus petit élément (au sens de l'ordre usuel $\leqslant$ sur $\mathbb{N}$) de $\varphi(x)$ ($\varphi(x) \neq \emptyset$ puisque $x \neq 0$) : on a bien $y \, \varepsilon \, x$ (car $y \in \varphi(x)$) et, si $t \, \varepsilon \, y$, alors $t < y$), donc, vu la façon dont y a été choisi, $t \notin \varphi(x)$, c'est-à-dire qu'on n'a pas $t \, \varepsilon \, x$.

b) Le fait que ζ est une bijection de l'ensemble des parties finies de $\mathbb{N}$ sur $\mathbb{N}$ se démontre sans difficulté, de même que le fait que, si x et y sont deux entiers, alors $x \in \zeta(y)$ implique $x < y$. D'après la question précédente, on voit donc que $\mathfrak{M}_0$ est un modèle de $ZF^- + AF$.

c) Il suffit de changer légèrement la définition de ζ. Considérons l'application ξ de W dans $\mathbb{N}$ définie par :

- si x est une partie finie de $\mathbb{N}$ différente de $\emptyset$ et de $\{0\}$, alors $\xi(x) = \zeta(x)$;
- $\xi(\emptyset) = 1$;
- $\xi(\{0\}) = 0$.

L'application ξ est encore bijective de W sur $\mathbb{N}$, et, d'après la question a), $\mathfrak{M}_{\xi^{-1}}$ est un modèle de ZF^-. En revanche, il ne satisfait pas AF puisque $0 \, \varepsilon_{\xi^{-1}} \, 0$ (voir 5.1).

2. Soient x un ordinal, y un sous-ensemble de x, transitif et distinct de x. D'après la proposition 2.3 et le corollaire 2.5, y, qui est un ensemble transitif d'ordinaux, est un ordinal ; $y \subseteq x$ signifie donc $y \leqslant x$, c'est-à-dire $y = x$ ou $y \in x$. La première éventualité étant exclue par hypothèse, on a nécessairement $y \in x$.

Réciproquement, soit x un ensemble de la classe On'. Il y a certainement des ordinaux qui ne sont pas inclus dans x (sinon, l'axiome de compréhension appliqué à l'ensemble $\mathfrak{P}(x)$ ferait de la classe des ordinaux un ensemble, ce qu'elle n'est pas). Désignons par β le premier des ordinaux non inclus dans x. On peut alors choisir un élément $\alpha \in \beta$ (qui sera évidemment un ordinal) tel que $\alpha \notin x$; α étant inférieur à β, on a, par définition de β, $\alpha \subseteq x$; de plus, α est un ensemble transitif (c'est un ordinal). Si α était distinct de x, on concluerait, parce que x est dans la classe On', que $\alpha \in x$, alors que α a été précisément choisi pour qu'il n'en soit pas ainsi. Il en résulte que $\alpha = x$, ce qui prouve que x est un ordinal.

3. Il suffit de reprendre la seconde démonstration du théorème 4.12 : on considère la classe des bons ordres sur les parties de x (qui est un ensemble par compréhension), puis on applique le schéma de remplacement pour montrer que $\Gamma(x)$ est un ensemble. Cet

ensemble est un ordinal, car c'est manifestement un ensemble transitif d'ordinaux (proposition 2.3 et corollaire 2.5). Il ne peut pas être subpotent à x, car cela impliquerait $\Gamma(x) \in \Gamma(x)$, ce qui est absurde, s'agissant d'un ordinal. Tout ordinal strictement inférieur à $\Gamma(x)$ appartient à $\Gamma(x)$, donc est subpotent à x. Il en résulte que $\Gamma(x)$ est le plus petit des ordinaux non subpotents à x. N'étant pas lui-même subpotent à x, $\Gamma(x)$ ne peut être équipotent à aucun ordinal subpotent à x, donc à aucun ordinal $\beta < \Gamma(x)$. Cela signifie que $\Gamma(x)$ est un cardinal.

On remarquera que, dans le théorème 4.12, l'ensemble qui jouait le rôle tenu ici par x était un ordinal, mais que cette propriété n'est nullement intervenue dans la preuve du résultat qui nous intéresse.

Si l'univers $\mathfrak{U}$ satisfait l'axiome du choix, x, comme n'importe quel ensemble, admet un cardinal (disons λ), qui est le plus grand des cardinaux subpotents à x. Comme $\Gamma(x)$ est un cardinal, et que c'est le plus petit des ordinaux non subpotents à x, on en conclut immédiatement que $\Gamma(x) = \lambda^+$

4. • AC $\Longrightarrow$ a) : soit a un ensemble et soit I l'ensemble des parties non vides de a ; considérons la famille $(a_i)_{i \in I}$ telle que, pour tout $i \in I$, $a_i = i$.

Par définition de I, tous les a_i sont non vides et, d'après AC, le produit $\prod_{i \in I} a_i$ est alors non vide ; soit x un élément de ce produit : x est une application de I dans $\bigcup_{i \in I} a_i$ telle que, pour tout $i \in I$, $x(i) \in a_i$; en remarquant que $\bigcup_{i \in I} a_i = a$, on voit donc que x est une application de I dans a telle que, pour toute partie non vide i de a, $x(i) \in i$, c'est-à-dire une fonction de choix sur a.

On remarquera qu'il est tout à fait possible que a soit l'ensemble vide et que, dans ce cas, il n'est pas nécessaire d'utiliser AC pour prouver l'existence d'une fonction de choix sur a : l'application vide convient parfaitement (l'ensemble des parties non vides de a est alors l'ensemble vide).

• a) $\Longrightarrow$ b) : soient x et y deux ensembles et g une surjection de x sur y. On considère une fonction de choix φ sur l'ensemble x et on définit une application h de y dans x de la manière suivante : pour chaque $t \in y$,

$$h(t) = \varphi(\bar{g}^{1}(\{t\}).$$

Cette définition est légitime parce que, g étant surjective, pour tout élément $t \in y$, l'image réciproque par g de $\{t\}$ est une partie non vide de x. Il est immédiat que, pour tout $t \in y$, $g(h(t)) = t$; $g \circ h$ est donc bien l'identité sur y.

• b) $\Longrightarrow$ c) : soit a un ensemble tel que, pour tous éléments x et y distincts appartenant à a, $x \neq \emptyset$ et $y \neq \emptyset$ et $x \cap y = \emptyset$; posons $w = \bigcup a$. Par hypothèse, pour chaque élément $t \in w$, il existe un unique élément $x \in a$ tel que $t \in x$. Nous pouvons poser $x = g(t)$, définissant ainsi une application g de w dans a, qui est surjective parce que l'ensemble vide n'appartient pas à a. D'après la condition b), il existe alors une application h de a dans w, telle que $g \circ h$ soit l'identité sur a. Désignons par b l'image de

cette application h, et remarquons que, pour tout $x \in a$, $h(x) \in x$ (parce que $x = g(h(x))$). On en déduit que, pour tout $x \in a$, $h(x) \in b \cap x$, et, pour tout élément y de a autre que x (et par là-même, d'après l'hypothèse, disjoint de x), $h(y) \notin x$. Cela prouve que, pour tout élément x de a, h(x) est l'unique élément de $b \cap x$: on a trouvé un ensemble dont l'intersection avec chaque élément de a est un singleton.

• c) $\Longrightarrow$ AC : soit $(a_i)_{i \in I}$ une famille d'ensembles non vides ; posons $b_i = \{i\} \times a_i$ pour chaque $i \in I$ et $a = \{b_i \, ; \, i \in I\}$. Les éléments de a sont non vides et deux à deux disjoints ; il existe donc un ensemble b tel que, pour tout $i \in I$, $b \cap b_i$ soit un singleton. Posons $c = \bigcup_{i \in I} a_i$ et $b' = b \cap (I \times C)$; on voit que, pour tout $i \in I$, il existe un et un seul élément de b' (l'unique élément de $b \cap b_i$) dont la première projection est i : b' est donc une application de I dans c, et, pour tout $i \in I$, b'(i), qui est la deuxième projection de l'unique élément de $b \cap b_i$, appartient à a_i : il s'agit donc d'un élément du produit de la famille $(a_i)_{i \in I}$, lequel est en conséquence non vide.

AC $\Longrightarrow$ d) : soient a et b deux ensembles. On utilise le théorème de Zermelo (théorème 3.3). On sait qu'il existe des ordinaux α et β équipotents respectivement à a et b. Par ailleurs, le corollaire 2.5 nous dit que α est inclus dans β (donc α est subpotent à β, ce qui implique que a est subpotent à b) ou β est inclus dans α (et dans ce cas β est subpotent à α, et b est subpotent à a).

d) $\Longrightarrow$ AC : cette fois encore, nous allons remplacer AC par le théorème de Zermelo qui lui est équivalent. On considère un ensemble x et on montre qu'il existe au moins un bon ordre sur x. On utilise le cardinal d'Hartog de x, défini dans l'exercice 3, noté $\Gamma(x)$, qui est le plus petit ordinal non subpotent à x. Puisque d) est supposé vérifié, il faut donc que ce soit x qui soit subpotent à $\Gamma(x)$. Soit φ une injection de x dans l'ordinal $\Gamma(x)$. Posons :

$$r = \{(u,v) \in x \times x \, ; \, \varphi(u) \subseteq \varphi(v)\}.$$

Une vérification routinière nous garantit que r est un bon ordre sur x : on n'a fait qu'« importer », par l'intermédiaire de l'injection φ, le bon ordre de l'ordinal $\Gamma(x)$.

5. On considère ici des ordres larges. Il est évident que, dans ZF, le théorème de Zermelo (et donc aussi l'axiome du choix) implique chacun des énoncés a), b) et c) (puisque n'importe quel ensemble est alors bien ordonnable). Toujours dans ZF, il va de soi que a) implique b), et on voit facilement que b) implique a) : soit (x,R) un ensemble bien ordonné, et soit α l'unique ordinal isomorphe à (x,R) ; l'isomorphisme entre α et x induit une bijection entre $\mathfrak{P}(\alpha)$ et $\mathfrak{P}(x)$; cette bijection permet de « transférer » un bon ordre sur $\mathfrak{P}(\alpha)$ (qui existe d'après b)) pour le transformer en un bon ordre sur $\mathfrak{P}(x)$. Montrons également que, dans ZF, c) implique b). Pour cela, il suffit de prouver que, pour tout ordinal α, l'ensemble $\mathfrak{P}(\alpha)$ est totalement ordonnable. Posons :

$r = \{(u,v) \in \mathfrak{P}(\alpha)^2 \, ;$ u = v ou le plus petit élément de la différence symétrique $u \, \Delta \, v$ appartient à u $\}$.

On vérifie sans peine que r est un ordre total sur $\mathfrak{P}(\alpha)$.

Nous allons montrer pour terminer que, dans ZF + AF, l'énoncé a) implique le théorème de Zermelo (et donc l'axiome du choix). Observons d'abord que, dans ZF + AF, le théorème de Zermelo équivaut à l'énoncé suivant :

(•) pour tout ordinal α, l'ensemble V_α est bien ordonnable.

En effet, il est clair que cet énoncé se déduit du théorème de Zermelo. Réciproquement, s'il est satisfait, étant donné un ensemble x quelconque, on peut choisir un ordinal α tel que $x \in V_\alpha$ (parce que l'axiome de fondation est satisfait) ; mais alors $x \subseteq V_\alpha$ (V_α est transitif) et, comme on peut trouver par hypothèse un bon ordre sur V_α, la restriction de ce bon ordre à x sera un bon ordre sur x.

Raisonnons alors par l'absurde en supposant que a) soit satisfait en même temps que la négation de (•). On peut alors considérer l'ordinal α minimum tel que V_α ne soit pas bien ordonnable, et on voit que α est nécessairement un ordinal limite (si $\alpha = \beta + 1$, alors $V_\alpha = \mathfrak{P}(V_\beta)$, V_β est bien ordonnable et V_α ne l'est pas, ce qui contredit a)).

On sait donc que, pour tout ordinal $\beta < \alpha$, il existe un bon ordre sur V_β ; on va utiliser a) pour montrer qu'il existe une famille $(s(\beta) \,;\, \beta < \alpha)$, où, pour chaque $\beta < \alpha$, $s(\beta)$ est un bon ordre sur V_β. Pour tout $\beta < \alpha$, posons : $X_\beta = \{\gamma \,;\, \gamma$ est l'ordinal d'un bon ordre sur $V_\beta\}$ (c'est un ensemble : voir la preuve de 4.12) ; posons ensuite : $X = \bigcup_{\beta \in \alpha} X_\beta$ et appelons δ la borne supérieure de X. Soit r un bon ordre sur $\mathfrak{P}(\delta)$ (il en existe d'après a)).

La famille $(s(\beta) \,;\, \beta < \alpha)$ est définie par induction.

• Si $\beta = 0$, il n'y a pas de problème : $s(\beta) = 0$.

• Si β est un ordinal limite, alors on sait que $V_\beta = \bigcup_{\gamma \in \beta} V_\gamma$. On vérifie alors que la relation $s(\beta)$ sur V_β définie comme suit est un bon ordre : pour tous éléments x, y de V_β, $x\, s(\beta)\, y$ si et seulement si :

- $rg(x) < rg(y)$ (voir en 5.2 la définition de rg)

ou - $rg(x) = rg(y)$, et, en posant $\gamma = rg(x)$, $x\, s(\gamma) y$ (remarquer que $\gamma < \beta$, et donc $s(\gamma)$ est déjà défini.

• Si β est un ordinal successeur, disons $\beta = \gamma + 1$, appelons δ_γ l'unique ordinal tel que $(V_\gamma, s(\gamma))$ soit isomorphe à $(\delta_\gamma, \in)$, et f_γ l'unique isomorphisme de $(V_\gamma, s(\gamma))$ sur $(\delta_\gamma, \in)$. Il est clair que $\delta_\gamma \leqslant \delta$, et f_γ induit une bijection g de V_β (qui est égal à $\mathfrak{P}(V_\gamma)$) sur $\mathfrak{P}(\delta_\gamma)$ (qui est inclus dans $\mathfrak{P}(\delta)$). On définit alors $s(\beta)$ en transférant l'ordre $r\restriction_{\mathfrak{P}(\delta_\gamma)}$ sur V_β : pour tous éléments x et y de V_β, $x\, s(\beta)\, y$ si et seulement si $g(x)\, r\, g(y)$.

Lorsqu'on dispose de la famille $(s(\beta) \,;\, \beta < \alpha)$, on peut définir un bon ordre s sur V_α par : pour tous éléments x, y de V_α, x s y si et seulement si :

- $rg(x) < rg(y)$

ou - $rg(x) = rg(y)$, et, en posant $\beta = rg(x)$, $x\, s(\beta)\, y$.

On aboutit donc à une contradiction.

6. On se référera au théorème de Cantor-Bernstein (4.2) par les initiales CB.

(1) $\Longrightarrow$ (2) : soient x un sous-ensemble dénombrable de a, φ une bijection de ω sur x, c l'image par φ de l'ensemble des entiers pairs, et b l'image par φ de l'ensemble des entiers impairs ; on définit une application f de a dans a comme suit : la restriction de f à $a - x$ est l'identité, et, pour tout ensemble $t \in x$, $f(t) = \varphi(2\varphi^{-1}(t))$; on vérifie facilement que f est une bijection de a sur $a - b$, et b est un sous-ensemble dénombrable de a.

(2) $\Longrightarrow$ (3) : soient b un ensemble dénombrable quelconque, x un sous-ensemble dénombrable de a, avec une bijection f de a sur $a - x$, et φ une bijection de b sur x ; l'application g, de $a \cup b$ dans a, qui coïncide avec φ sur b et avec f sur $a - (a \cap b)$ est clairement une injection ; par ailleurs, l'identité est évidemment une injection de a dans $a \cup b$; on en déduit que a et $a \cup b$ sont équipotents (CB).

(3) $\Longrightarrow$ (4) : soient x un ensemble fini et b un ensemble dénombrable contenant x (par exemple $\omega \cup x$) ; on a une bijection de $a \cup b$ dans a, dont la restriction à $a \cup x$ est une injection de $a \cup x$ dans a ; comme l'identité est une injection de a dans $a \cup x$, on en conclut que a et $a \cup x$ sont équipotents (CB).

(4) $\Longrightarrow$ (5) : soient x un sous-ensemble fini de a, y un ensemble équipotent à x et disjoint de a, et f une bijection de $a \cup y$ sur a ; appelons z l'image directe de y par f et posons : $t = x \cap z$, $u = x - t$, $v = z - t$ et $w = a - (x \cup z)$; on vérifie facilement que les ensembles t, u, v et w constituent une partition de a, que x et z sont équipotents, de même que u et v ; choisissons une bijection φ de u sur v, et considérons l'application h, de a dans a, qui coïncide avec l'identité sur $w \cup t$, avec φ sur u, et avec φ^{-1} sur v ; h est une bijection de a sur a qui échange x et z, et l'application composée $g = h \circ f$ est une bijection de $a \cup y$ sur a telle que l'image de y soit x et l'image de a soit $a - x$; la restriction de g à a est une bijection de a sur $a - x$: ces deux ensembles sont équipotents.

(5) $\Longrightarrow$ (6) : évident (n'importe quel entier non nul convient).

(6) $\Longrightarrow$ (7) : puisque a est non vide, il résulte de (6) que, pour tout sous-ensemble y de a à un élément, a et $a - y$ sont équipotents ; considérons un tel sous-ensemble, par exemple $y = \{t\}$, où $t \in a$, et une bijection f de a sur $a - y$; soit maintenant x un ensemble quelconque à un élément, disons $x = \{u\}$; évidemment, si $u \in a$, l'équipotence entre a et $a \cup x$ n'est pas difficile à établir ... ; si $u \notin a$, l'application g de $a \cup x$ dans a qui coïncide avec f sur a et qui à u associe t est une bijection, ce qui montre que $a \cup x$ et a sont équipotents et prouve (7) (avec $n = 1$, c'est-à-dire, en fait, (8) !).

(7) $\Longrightarrow$ (8) : soient n (> 0) un entier donné par (7), t un ensemble quelconque, et y un ensemble de cardinal $n - 1$ (par exemple $n - 1$ lui-même) ; posons $x = y \cup \{t\}$; on a alors $a \subseteq a \cup \{t\} \subseteq a \cup x$, et (d'après (7)) a est équipotent à $a \cup x$; cela prouve que a et $a \cup \{t\}$ sont équipotents (CB).

(8) $\Longrightarrow$ (9) : choisissons un ensemble u tel que $u \notin a$; soit f une bijection de $a \cup \{u\}$ sur a, et posons $t = f(u)$; on voit que la restriction de f à a est une bijection de a sur $a - \{t\}$, ces deux ensembles sont donc équipotents.

(9) $\Longrightarrow$ (10) : soit t un ensemble tel que $t \in a$ et tel que a soit équipotent à $b = a - \{t\}$; a n'étant pas vide, b, qui lui est équipotent, ne l'est pas non plus ; d'autre part $b \neq a$ parce que $t \in a$ et $t \notin b$; b est donc une partie de a, non vide, distincte de a, et équipotente à a.

(10) $\Longrightarrow$ (11) : évident (« équipotent » est plus fort que « subpotent »).

(11) $\Longrightarrow$ (1) : on considère un ensemble b tel que $b \subsetneq a$, $b \neq \emptyset$, $b \neq a$, et a est subpotent à b ; soit f une injection de a dans b ; on définit une suite $(x_n)_{n \in \omega}$ d'éléments de a, par induction sur les entiers, comme suit : x_0 est un élément arbitraire de l'ensemble $a - b$ (il y en a) et, pour tout $n \in \omega$, $x_{n+1} = f(x_n)$; désignons par c l'image de cette suite ($c = \{t \in a ; (\exists n \in \omega)(t = x_n)\}$), et montrons que c est un ensemble dénombrable ; pour cela, il nous suffit de prouver que, pour tous entiers n et m distincts, $x_n \neq x_m$; supposons que ce ne soit pas vrai, et appelons k le plus petit élément de l'ensemble (alors non vide) suivant : $Z = \{n \in \omega ; (\exists m \in \omega)(m > n \wedge x_m = x_n)\}$; soit h un entier tel que $h > k$ et $x_h = x_k$; si $k \neq 0$, on a $x_h = f(x_{h-1}) = x_k = f(x_{k-1})$, et, parce que f est injective, $x_{h-1} = x_{k-1}$, ce qui prouve que $k - 1 \in Z$ et contredit la définition de k ; on en déduit que $k = 0$, mais cela aussi mène à une contradiction car $x_0 \notin b$, tandis que x_h, qui est un élément de l'image de f (puisque $h > 0$), appartient à b, ce qui interdit l'égalité $x_0 = x_k$.

Le lecteur perspicace aura compris que les ensembles qui satisfont une des onze propriétés dont nous venons de prouver l'équivalence sont les ensembles infinis. Il conviendrait de préciser infinis **au sens fort**, un ensemble infini **au sens faible** étant un ensemble qui n'est équipotent à aucun entier. Ces deux notions n'en font qu'une lorsque l'univers satisfait l'axiome du choix, mais, en l'absence de celui-ci, rien ne prouve qu'un ensemble qui n'est équipotent à aucun entier doive contenir un sous-ensemble dénombrable.

7. Pour cet exercice et les trois suivants, nous nous contenterons de donner les réponses, avec éventuellement des indications sommaires. Le lecteur pourra (avec profit) faire les preuves complètes.

On utilise les faits suivants :

- $\text{card}(\mathfrak{P}(\mathbb{N})) = \text{card}(\mathbb{N}^{\mathbb{N}}) = \text{card}(\mathbb{Q}^{\mathbb{N}}) = \text{card}(\mathbb{R}) = \text{card}(\mathbb{R}^{\mathbb{N}}) = 2^{\aleph_0}$;
- l'ensemble $\mathfrak{P}_f(\mathbb{N})$ des parties finies de $\mathbb{N}$ est dénombrable ;
- l'ensemble $\mathfrak{P}_\infty(\mathbb{N})$ des parties infinies de $\mathbb{N}$ est de cardinal $2^{\aleph_0}$.

$\text{card}(x_1) = 2^{\aleph_0}$: à chaque partie infinie de $\mathbb{N}$, on associe la suite de ses éléments pris dans l'ordre croissant, ce qui donne une bijection de $\mathfrak{P}_\infty(\mathbb{N})$ sur x_1, qui est l'ensemble des suites d'entiers strictement croissantes ;

$\text{card}(x_2) = 2^{\aleph_0}$: x_2 est l'ensemble des suites d'entiers bornées, il contient l'ensemble $2^{\mathbb{N}}$;

$\text{card}(x_3) = 2^{\aleph_0}$: x_3 est l'ensemble des suites de rationnels strictement croissantes, il contient x_1 ;

$\text{card}(x_4) = 2^{\aleph_0}$: x_4 est l'ensemble des suites de rationnels bornées, il contient x_2 ;

$\text{card}(x_5) = 2^{\aleph_0}$: à chaque élément $f \in x_1$, on associe l'application g de $\mathbb{N}$ dans $\mathbb{Q}$ qui, à chaque entier n, associe $-\dfrac{1}{1 + f(n)}$;

g est une suite strictement croissante et bornée de rationnels, et on a ainsi une injection de x_1 dans x_5 ;

$\text{card}(x_6) = \aleph_0$: pour chaque $n \in \mathbb{N}$, on pose :

$$z_n = \{f \in \mathbb{Q}^{\mathbb{N}} ; (\forall p \in \mathbb{N})(n \leqslant p \Longrightarrow f(n) = f(p))\} ;$$

on a donc $x_6 = \bigcup_{n \in \mathbb{N}} z_n$; or chacun des z_n est équipotent à $\mathbb{Q}^{n+1}$; on en déduit que x_6 est équipotent à $\bigcup_{n \in \mathbb{N}} \mathbb{Q}^{n+1}$, ensemble qui est dénombrable (théorème 4.9, 3°)) ;

$\text{card}(x_7) = 2^{\aleph_0}$: x_7 est l'ensemble des suites de réels non bornées ; il contient x_1.

8. $\text{card}(E_0) = \text{card}(\mathbb{N}^{\mathbb{N}}) = 2^{\aleph_0}$;

$\text{card}(E_1) = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0^2} = 2^{\aleph_0}$;

$\text{card}(E_2) = 2^{\aleph_0}$: utiliser le fait que l'ensemble des suites strictement croissantes d'entiers naturels est de cardinal $2^{\aleph_0}$ (voir l'exercice 7) ; à une telle suite u, faire correspondre la suite de rationnels v définie par $v(n) = \dfrac{1}{1 + u(n)}$ pour tout n ;

$\text{card}(E_3) = 2^{\aleph_0}$: $E_2 \subseteq E_3 \subseteq E_0$;

$\text{card}(E_4) = 2^{\aleph_0}$: $E_2 \subseteq E_4 \subseteq E_0$;

$\text{card}(E_5) = 2^{\aleph_0}$: toute suite strictement croissante d'entiers naturels est une suite non bornée de rationnels, et $E_5 \subseteq E_0$;

$\text{card}(E_6) = \text{card}(E_1) = 2^{\aleph_0}$;

$\text{card}(E_7) = \text{card}(E_6) = 2^{\aleph_0}$: si deux applications continues de $\mathbb{R}$ dans $\mathbb{R}$ ont même restriction à $\mathbb{Q}$, alors elles sont égales ;

$\text{card}(E_8) = 2^{\aleph_0}$: E_8 est évidemment subpotent à $\mathbb{R} \times \mathbb{R}$;

$\text{card}(E_9) = 2^{\aleph_0}$: on utilise le résultat classique suivant : tout ouvert de $\mathbb{R}$ est réunion d'une famille d'intervalles ouverts deux à deux disjoints, indexée par l'ensemble des entiers naturels ; on en déduit l'existence d'une injection de E_9 dans $(E_8)^{\mathbb{N}}$.

9. Nous appellerons suites les applications de ω dans ω.

$\text{card}(a_1) = 1$: a_1 ne contient que la suite nulle ;

$\text{card}(a_2) = 2^{\aleph_0}$: a_2 est égal à ω^ω (prendre $p = f(n)$) ;

$\text{card}(a_3) = 2^{\aleph_0}$: a_3 est l'ensemble des suites qui prennent au moins une fois la valeur 0 ; il contient l'ensemble des suites f telles que $f(0) = 0$, qui est équipotent à $\omega^{\omega - \{0\}}$;

$\text{card}(a_4) = 2^{\aleph_0}$: $a_2 \subseteq a_4 \subseteq \omega^\omega$ (en fait, $a_4 = \omega^\omega$) ;

$\text{card}(a_5) = 2^{\aleph_0}$: a_5 est l'ensemble des suites bornées, il contient 2^ω ;

$\text{card}(a_6) = 2^{\aleph_0}$: $a_3 \subseteq a_6 \subseteq \omega^\omega$ (en fait, $a_6 = a_3$) ;

$\text{card}(b_1) = 0$: toute suite satisfait la négation de la propriété indiquée ;

$\text{card}(b_2) = 2^{\aleph_0}$: b_2 est égal à ω^ω (prendre $p = f(n)$) ;

$\text{card}(b_3) = 0$: toute suite satisfait la négation de la propriété indiquée ;

$\text{card}(b_4) = 2^{\aleph_0}$: $b_2 \subseteq b_4 \subseteq \omega^\omega$ (en fait, $b_4 = \omega^\omega$) ;

$\text{card}(b_5) = 2^{\aleph_0}$: $b_5 = \omega^\omega$ (prendre $p = 0$) ;

$\text{card}(b_6) = 2^{\aleph_0}$: b_6 est l'ensemble des suites non bornées, il contient l'ensemble des suites strictement croissantes (x_1 dans l'exercice 7).

10. $\text{card}(y_1) = \mu$: à chaque élément $x \in b$, on associe l'application de a dans b qui prend en tout point la valeur x ; on définit ainsi une bijection de b sur y_1 ;

$\text{card}(y_2) = \mu$: y_2 est égal à y_1, car, pour tout $x \in \mathfrak{P}(a)$, et pour tout $f \in b^a$, on a $\text{card}(\bar{f}(x)) \leqslant \text{card}(\bar{f}(a))$, ce qui montre que $y_1 \subseteq y_2$, et, d'autre part, si $f \in y_2$, on a $\text{card}(\bar{f}(a)) \leqslant 1$, donc $\text{card}(\bar{f}(a)) = 1$, puisque a est non vide, ce qui prouve que $y_2 \subseteq y_1$;

$\text{card}(y_3) = 2^\lambda$: pour toute application f de a dans b, on a $\bar{f}^{-1}(b) = a$, donc $\text{card}(\bar{f}^{-1}(b)) = \lambda$; cela montre que $y_3 = b^a$ et que $\text{card}(y_3) = \mu^\lambda = 2^\lambda$ (puisque $2 \leqslant \mu \leqslant \lambda$) ;

$\text{card}(y_4) = 2^\lambda$: soient x et y deux éléments distincts de b (b est infini) ; on a $\{x,y\}^a \subseteq y_4 \subseteq b^a$, donc $2^\lambda \leqslant \text{card}(y_4) \leqslant \mu^\lambda = 2^\lambda$;

$\text{card}(y_5) = \lambda$: comme g est injective, le cardinal de $\bar{g}(b)$ est celui de b, c'est-à-dire μ ; comme a est de cardinal $\lambda > \mu$, la différence $a - \bar{g}(b)$ est de cardinal λ (proposition 4.14) ;

$\text{card}(y_6) = 2^\lambda$: en associant à chaque élément de y_6 sa restriction à l'ensemble y_5, on obtient une bijection de y_6 sur b^{y_5} ;

$\text{card}(y_7) = 2^\lambda$: tout élément de y_6 est une application surjective de a sur b, donc un élément de y_7 ; on en déduit que $y_6 \subseteq y_7 \subseteq b^a$.

11. a) Soit n un entier naturel non nul. Posons $b = a \times n$. On a $\text{card}(b) = \lambda$ (corollaire 4.14). On peut donc choisir une application bijective h de b sur a. Pour chaque $i \in \{1,2,\ldots,n\}$ désignons par a_i l'image par h du sous-ensemble $a \times \{i-1\}$ de b ; le

cardinal de chaque a_i est évidemment λ, et les a_i $(1 \leqslant i \leqslant n)$ constituent une partition de a.

b) Pour tout $x \in \mathfrak{P}(a)$, on a $\text{card}(a) = \sup(\text{card}(x), \text{card}(a - x))$ (corollaire 4.14) ; donc, si $x \in \mathfrak{P}^*(a)$, $\text{card}(x) = \lambda$.

c) Considérons une partition de a en trois parties a_1, a_2, a_3, toutes de cardinal λ, comme nous y autorise la question a). L'application $x \longmapsto a_2 \cup x$, de $\mathfrak{P}(a_1)$ dans $\mathfrak{P}(a)$ est injective, et son image est un sous-ensemble de $\mathfrak{P}^*(a)$, car, si $x \subseteq a_1$, alors les inclusions $a_2 \subseteq a_2 \cup x \subseteq a$ et $a_3 \subseteq a - (a_2 \cup x) \subseteq a$ prouvent que $\text{card}(a_2 \cup x) = \text{card}(a - (a_2 \cup x)) = \lambda$. On a donc $\text{card}(\mathfrak{P}(a_1)) \leqslant \text{card}(\mathfrak{P}^*(a)) \leqslant \text{card}(\mathfrak{P}(a))$. Conclusion : $\text{card}(\mathfrak{P}^*(a)) = 2^\lambda$.

d) Soit $a_1 \in \mathfrak{P}^*(a)$, et posons $b = a - a_1$. Comme $\text{card}(b) = \lambda$, on peut trouver une partition de b en deux parties b_1 et b_2, chacune de cardinal λ (question a)). Les ensembles a_1, b_1 et b_2 constituent une partition de a. Choisissons une bijection φ de b_1 sur b_2, et définissons comme suit une application h_{a_1} de a dans a :

- la restriction de h_{a_1} à a_1 est l'identité ;
- la restriction de h_{a_1} à b_1 est l'application φ ;
- la restriction de h_{a_1} à b_2 est l'application φ^{-1}.

On vérifie facilement que h_{a_1} est une bijection de a sur a dont l'ensemble des points invariants est a_1 (pour $x \in b_1$, $h_{a_1}(x) \in b_2$, donc $h_{a_1}(x) \neq x$; le raisonnement est le même si $x \in b_2$).

e) La question précédente montre que l'application $a_1 \longmapsto h_{a_1}$ est une injection de $\mathfrak{P}^*(a)$ dans l'ensemble $S(a)$ des bijections de a sur a. Comme $S(a)$ est inclus dans l'ensemble de toutes les applications de a dans a, on en déduit que :

$$2^\lambda \leqslant \text{card}(S(a)) \leqslant \lambda^\lambda = 2^\lambda.$$

Le cardinal de l'ensemble des bijections de a sur a est donc 2^λ.

f) Soit $b \in \mathfrak{P}^*(a)$, et soit X l'ensemble des bijections de a sur a dont la restriction à b est l'identité sur b. On définit une bijection de X sur $S(a - b)$ (ensemble des bijections de $a - b$ sur $a - b$) en associant à chaque élément de X sa restriction à $a - b$. Le cardinal de X est donc celui de $S(a - b)$, c'est-à-dire 2^λ, puisque $\text{card}(a - b) = \lambda$ (voir la question e)).

g) A toute bijection f de a sur a, on peut associer une application φ_f, injective, de a dans $\mathfrak{P}(a)$, en posant $\varphi_f(x) = \{f(x)\}$ pour tout $x \in a$. On voit tout de suite que l'application $f \longmapsto \varphi_f$ est une injection de $S(a)$ dans l'ensemble des applications injectives de a dans $\mathfrak{P}(a)$, qui est lui même une partie de $\mathfrak{P}(a)^a$. Or $\text{card}(S(a)) = 2^\lambda$ et $\text{card}(\mathfrak{P}(a)^a) = (2^\lambda)^\lambda = 2^{\lambda \times \lambda} = 2^\lambda$. Le cardinal cherché est donc 2^λ.

12. On va définir, par induction sur $\beta \in \alpha$, une famille $(f_\beta)_{\beta\in\alpha}$ d'injections de X_β dans λ telle que, pour tous ordinaux $\beta \in \alpha$ et $\gamma \in \alpha$, si $\beta < \gamma$, alors $f_\beta \subseteq f_\gamma$:

• f_0 est une injection arbitraire de X_0 dans λ (il y en a car $\text{card}(X_0) < \lambda$) ;

• si $\beta \in \alpha$ et β est un ordinal limite, on pose $f_\beta = \bigcup_{\gamma\in\beta} f_\gamma$;

• si $\beta \in \alpha$ et $\beta = \gamma + 1$, on définit f_β comme suit : la restriction de f_β à X_γ est f_γ et la restriction de f_β à $X_{\gamma+1} - X_\gamma$ est une injection de $X_{\gamma+1} - X_\gamma$ dans λ dont l'image est disjointe de celle de f_γ. Une telle injection existe parce que : l'image de f_γ est un sous-ensemble de λ de cardinal $\text{card}(X_\gamma) < \lambda$, donc $\text{card}(\lambda - \text{Im}(f_\gamma)) = \lambda > \text{card}(X_{\gamma+1} - X_\gamma))$; de plus, l'axiome du choix est satisfait.

On vérifie facilement que la famille d'applications ainsi définie a les propriétés requises. L'application $f = \bigcup_{\beta\in\alpha} f_\beta$ est une injection de $\bigcup_{\beta\in\alpha} X_\beta$ dans λ.

Conclusion : $\text{card}(\bigcup_{\beta\in\alpha} X_\beta) \leqslant \lambda$.

13. Par définition, $\sum_{\alpha\in\kappa} \lambda_\alpha = \text{card}(\bigcup_{\alpha\in\kappa} (\lambda_\alpha \times \{\alpha\}))$.

Avec le corollaire 4.14, 2°), on en déduit que : $\sum_{\alpha\in\kappa} \lambda_\alpha \leqslant \sup(\kappa, \sup_{\alpha\in\kappa} \lambda_\alpha)$.

Pour obtenir l'inégalité inverse, on fait les deux remarques suivantes :

• l'application $\alpha \longmapsto (0,\alpha)$ est une injection de κ dans $\bigcup_{\alpha\in\kappa} (\lambda_\alpha \times \{\alpha\})$;

• l'application de $\bigcup_{\alpha\in\kappa} \lambda_\alpha = \sup_{\alpha\in\kappa} \lambda_\alpha$ dans $\bigcup_{\alpha\in\kappa} (\lambda_\alpha \times \{\alpha\})$ qui, à tout élément x, associe l'unique couple (x,α) tel que $\alpha \in \kappa$, $x \in \lambda_\alpha$ et, pour tout $\beta < \alpha$, $x \notin \lambda_\beta$, est également injective.

Il en résulte que $\kappa \leqslant \sum_{\alpha\in\kappa} \lambda_\alpha$ et $\sup_{\alpha\in\kappa} \lambda_\alpha \leqslant \sum_{\alpha\in\kappa} \lambda_\alpha$.

Finalement : $\sum_{\alpha\in\kappa} \lambda_\alpha = \sup(\kappa, \sup_{\alpha\in\kappa} \lambda_\alpha)$.

14. a) On a $2 \leqslant \mu \leqslant \lambda$, donc $2^\lambda \leqslant \mu^\lambda \leqslant \lambda^\lambda = 2^\lambda$, ce qui montre que $2^\lambda = \mu^\lambda = \lambda^\lambda$. D'autre part, $\aleph_0 \leqslant \mu \leqslant \lambda$, donc $\lambda^{\aleph_0} \leqslant \lambda^\lambda = 2^\lambda$. Il suffit de montrer que $2^\lambda \leqslant \lambda^{\aleph_0}$. Pour cela, on vérifie que :

$$(\bullet) \qquad 2^\lambda = \prod_{n\in\omega} 2^{\lambda_n},$$

et on remarque que, pour tout $n \in \omega$, $2^{\lambda_n} \leqslant \lambda$.

Pour montrer $(\bullet)$, on se donne une famille $(X_n)_{n\in\omega}$ d'ensembles deux à deux disjoints telle que, pour tout n, X_n soit de cardinal λ_n, et on pose $X = \bigcup_{n\in\omega} X_n$. Le cardinal de X est λ, donc celui de $\mathfrak{P}(X)$ est 2^λ. A chaque partie $Y \subseteq X$, on fait correspondre la suite $(Y_n)_{n\in\omega}$ telle que, pour tout n, $Y_n = Y \cap X_n$. On a ainsi une application, qui est clairement bijective (parce que les X_n sont deux à deux disjoints), de $\mathfrak{P}(X)$ dans $\prod_{n\in\omega} \mathfrak{P}(X_n)$, ce qui donne bien $(\bullet)$.

b) Soit γ un cardinal.

• si γ est compris entre $\aleph_0$ et λ (au sens large), alors :

$$\lambda^{\aleph_0} \leqslant \lambda^\gamma \leqslant \lambda^\lambda = 2^\lambda ;$$

mais on vient de voir que $2^\lambda \leqslant \lambda^{\aleph_0}$, ce qui prouve les égalités $\lambda^{\aleph_0} = \lambda^\gamma = \lambda^\lambda$.

• si γ est supérieur ou égal à λ , on a $2 \leqslant \lambda \leqslant \gamma$, donc :

$$2^\gamma \leqslant \lambda^\gamma \leqslant \gamma^\gamma = 2^\gamma.$$

c) Il suffit de choisir : $\alpha = \delta = \lambda$, $\beta = 2^\lambda$, et $\gamma = \aleph_0$. On a bien $\alpha < \beta$ et $\gamma < \delta$ (la première inégalité résulte du théorème de Cantor (4.5), la deuxième du fait que $\mu \geqslant \aleph_0$ et $\lambda \geqslant 2^\mu \geqslant 2^{\aleph_0} > \aleph_0$). Calculons α^γ et β^δ :

• $\alpha^\gamma = \lambda^{\aleph_0} = \lambda^\lambda = 2^\lambda$ (question b)) ;

• $\beta^\delta = (2^\lambda)^\lambda = 2^{\lambda \times \lambda} = 2^\lambda$.

On en déduit l'égalité attendue.

15. a) Pour tout ordinal α, α est cofinal à α: l'identité est une application strictement croissante non strictement majorée de α dans α (c'est vrai même si $\alpha = 0$: l'identité est alors l'application vide qui a aussi ces propriétés). La relation est donc réflexive. Pour prouver la transitivité, considérons des ordinaux α, β et γ tels que α soit cofinal à β et β cofinal à γ; il y a donc des applications $f : \beta \longrightarrow \alpha$ et $g : \gamma \longrightarrow \beta$, strictement croissantes et non strictement majorées. Alors, $f \circ g$ est une application de γ dans α qui est strictement croissante. Montrons qu'elle n'est pas strictement majorée : soit δ un élément de α; on peut trouver un élément $\xi \in \beta$ tel que $f(\xi) \geqslant \delta$, puis un élément $\zeta \in \gamma$ tel que $g(\zeta) \geqslant \xi$; comme f est croissante, on a :

$$(f \circ g)(\zeta) = f(g(\zeta)) \geqslant f(\xi) \geqslant \delta.$$

L'ordinal $\aleph_\omega$ est cofinal à ω: l'application $n \longmapsto \aleph_n$ de ω dans $\aleph_\omega$ est en effet strictement croissante et n'est pas strictement majorée. Mais ω n'est pas cofinal à $\aleph_\omega$, car il ne peut exister d'application injective (et a fortiori d'application strictement croissante) de $\aleph_\omega$ dans ω. La relation « être cofinal à » n'est donc pas symétrique.

Les ordinaux cofinaux à 1 sont les ordinaux successeurs : si $\alpha = \beta + 1$ est successeur, alors l'application f de 1 ($= \{0\}$) dans α, définie par $f(0) = \beta$ est strictement croissante et n'est pas strictement majorée (pour tout $\gamma \in \alpha$, $f(0) \geqslant \gamma$), donc α est cofinal à 1 ; réciproquement, si α est un ordinal cofinal à 1, et si g est une application de 1 dans α qui n'est pas strictement majorée, on doit avoir (parce que 0 est le seul élément de 1) : $f(0) \geqslant \delta$ pour tout $\delta \in \alpha$; cela signifie que $f(0)$ doit être le plus grand élément dans α ; cette situation n'est possible que si α est successeur.

b) Si α et β sont des ordinaux tels que α soit cofinal à β, alors l'existence d'une application strictement croissante de β dans α, prouve que β est inférieur ou égal à α. La classe des ordinaux β tels que α soit cofinal à β est donc l'ensemble : $\{\beta \in \alpha + 1 ; \alpha$ est cofinal à $\beta\}$ (axiome de compréhension). Cet ensemble n'est pas vide car il contient α ; son plus petit élément, $\mathrm{cof}(\alpha)$, est donc inférieur ou égal à α. Soit γ un ordinal tel que

$\text{cof}(\alpha)$ soit cofinal à γ ; par transitivité, α est alors cofinal à γ, ce qui prouve que $\text{cof}(\alpha) \leqslant \gamma$: $\text{cof}(\alpha)$ est donc le plus petit des ordinaux auxquels $\text{cof}(\alpha)$ est cofinal, ce qui signifie que $\text{cof}(\text{cof}(\alpha)) = \text{cof}(\alpha)$, ou encore que $\text{cof}(\alpha)$ est régulier.

c) Supposons d'abord que $\beta \geqslant \text{cof}(\alpha)$. Choisissons une application f strictement croissante non strictement majorée de $\text{cof}(\alpha)$ dans α. Alors, l'application g de β dans α qui coïncide avec f sur le sous-ensemble $\text{cof}(\alpha)$ de β, et qui vaut **0** en dehors de ce sous-ensemble, n'est pas strictement majorée dans α.

Réciproquement, supposons qu'il existe une application f de β dans α, non strictement majorée dans α. Cela signifie que la borne supérieure de l'image de f est l'ordinal α. Appelons δ le premier ordinal de l'ensemble :

$$\{\gamma \leqslant \beta\,;\ \sup_{\xi \in \gamma} f(\xi) = \alpha\}.$$

(Cet ensemble n'est pas vide car, comme nous venons de le voir, il contient β.) On définit alors une application g de δ dans α, comme suit : pour tout $\gamma \in \delta$,

$$g(\gamma) = \sup_{\xi \in \gamma} f(\xi).$$

Il est facile de vérifier que g est croissante. La définition de δ nous garantit, d'une part qu'elle prend bien ses valeurs dans α, et, d'autre part, qu'elle n'est pas strictement majorée dans α. Désignons par X l'image de g, et par h l'application de X dans δ qui, à chaque ordinal $x \in X$, associe le plus petit des ordinaux ξ tels que $x = g(\xi)$. On se convainc facilement que h est un isomorphisme de X (muni de l'ordre $\in$) sur son image, qui est un sous-ensemble Y de δ ; Y est isomorphe à un (unique) ordinal $\sigma \leqslant \delta$ (remarque 2.6). Soit φ l'isomorphisme de Y sur σ. On voit que $(\varphi \circ h)^{-1}$, isomorphisme de σ sur X, est une application strictement croissante non strictement majorée de σ dans α. On en déduit que α est cofinal à σ. En conséquence, β, qui vérifie $\beta \geqslant \delta \geqslant \sigma$, est supérieur ou égal à la cofinalité de α.

d) Comme tous les ordinaux successeurs sont cofinaux à 1 (question a)), le seul ordinal successeur qui puisse être régulier est 1 ; il l'est effectivement, car toute application de 0 dans 1 est majorée (par 0), ce qui montre que 1 n'est pas cofinal à 0. L'unique ordinal successeur régulier est bien un cardinal. Comme 0 est cofinal à 0, il est régulier ; c'est aussi un cardinal. Il nous reste à examiner le cas des ordinaux réguliers limites. Soit α un tel ordinal et soit λ le cardinal de α. Bien entendu, $\lambda \leqslant \alpha$, et on peut choisir une bijection f de λ sur α. Comme α est limite, f n'est pas strictement majorée dans α. Grâce à la question c), on en déduit que $\lambda \geqslant \text{cof}(\alpha) = \alpha$. Conclusion : $\lambda = \alpha$ et α est un cardinal. Ainsi, tout ordinal régulier est un cardinal.

Soit λ un cardinal qui est un ordinal régulier, et soit X un sous-ensemble de λ tel que $\text{card}(X) < \lambda$. Muni du bon ordre $\in$, X est isomorphe à un ordinal $\delta \leqslant \lambda$ (remarque 2.6) ; mais cette inégalité ne peut être que stricte puisque $\text{card}(\delta) = \text{card}(X) < \lambda$ et que λ est lui-même un cardinal. Soit φ l'isomorphisme de δ sur X ; φ est une application strictement croissante de $\delta < \lambda$ dans λ qui est régulier. On en déduit immédiatement que

φ est strictement majorée dans λ, ce qui signifie exactement que la borne supérieure de l'ensemble X est strictement inférieure à λ. Donc λ est un cardinal régulier au sens de la définition 5.7, ii. Réciproquement, supposons que λ soit un cardinal régulier au sens de 5.7, ii, et considérons un ordinal $\alpha < \lambda$ et une application f strictement croissante de α dans λ. L'image de f est un sous-ensemble Y de λ dont le cardinal est strictement inférieur à λ, puisque c'est le même que celui de α. On en déduit que la borne supérieure de Y est un élément de λ, ce qui montre que l'application f est strictement majorée dans λ : λ n'est donc pas cofinal à α ; c'est un ordinal régulier.

e) On suppose maintenant que l'univers satisfait l'axiome du choix. Soit α un ordinal et appelons λ la cofinalité de $\aleph_{\alpha+1}$. Il existe une application f, strictement croissante et non strictement majorée, de λ dans $\aleph_{\alpha+1}$. Pour tout $\beta \in \lambda$, $f(\beta) \in \aleph_{\alpha+1}$, c'est-à-dire $f(\beta) < \aleph_{\alpha+1}$, donc $\text{card}(f(\beta)) \leqslant \aleph_\alpha$. D'autre part, comme f n'est pas strictement majorée dans $\aleph_{\alpha+1}$ qui est un ordinal limite, on a :

$$\aleph_{\alpha+1} = \sup_{\beta\in\lambda} f(\beta) = \bigcup_{\beta\in\lambda} f(\beta).$$

On en déduit que :

$$\text{card}(\bigcup_{\beta\in\lambda} f(\beta)) = \aleph_{\alpha+1}.$$

Mais, par ailleurs, on a aussi (corollaire 4.14, 2°, avec AC) :

$$\text{card}(\bigcup_{\beta\in\lambda} f(\beta)) \leqslant \sup(\lambda, \sup_{\beta\in\lambda} \text{card}(f(\beta))).$$

En conséquence, $\aleph_{\alpha+1} \leqslant \sup(\lambda, \sup_{\beta\in\lambda}\text{card}(f(\beta)))$; or, pour pour tout $\beta \in \lambda$, $\text{card}(f(\beta)) \leqslant \aleph_\alpha$, donc $\sup_{\beta\in\lambda}\text{card}(f(\beta)) \leqslant \aleph_\alpha < \aleph_{\alpha+1}$, ce qui implique $\lambda \geqslant \aleph_{\alpha+1}$. Mais $\lambda = \text{cof}(\aleph_{\alpha+1}) \leqslant \aleph_{\alpha+1}$. Conclusion : $\aleph_{\alpha+1}$ est régulier.

Supposons que α soit un ordinal limite, et appelons δ sa cofinalité. Soit f une application strictement croissante de δ dans α, non strictement majorée. Alors l'application g de δ dans $\aleph_\alpha$ qui à $\beta \in \delta$ fait correspondre $\aleph_{f(\beta)}$ est aussi strictement croissante, non strictement majorée, ce qui montre que $\aleph_\alpha$ est cofinal à δ et que $\text{cof}(\aleph_\alpha) \leqslant \delta$. Pour montrer que $\text{cof}(\aleph_\alpha) = \delta$, on va utiliser la question c), et montrer que, si β est un ordinal strictement inférieur à δ et si h est une application de β sur $\aleph_\alpha$, alors h est strictement majorée dans $\aleph_\alpha$. En effet, considérons l'application k de domaine β qui à $\gamma \in \beta$ fait correspondre l'unique ordinal ε tel que $\aleph_\varepsilon$ soit la cardinalité de $h(\gamma)$; k est en fait une application de β dans α, et d'après la question c), puisque β est strictement inférieur à la cofinalité de α, k est majorée par un ordinal $\zeta < \alpha$. On en déduit que, pour tout $\gamma \in \beta$, $h(\gamma) < \aleph_{\zeta+1}$. Comme α est un ordinal limite, $\zeta + 1 < \alpha$ et $\aleph_{\zeta+1} < \aleph_\alpha$: h est donc strictement majorée dans $\aleph_\alpha$.

f) L'application $n \longmapsto \omega + n$ de ω dans $\omega + \omega$ (il s'agit de sommes ordinales) est clairement strictement croissante et non strictement majorée. On en déduit que $\omega + \omega$ est cofinal à ω. Il est d'autre part évident qu'aucun des ordinaux $\omega + n$ $(0 < n < \omega)$ n'est cofinal à ω : toute application strictement croissante de ω dans $\omega + n$ est strictement

majorée par ω. Le plus petit ordinal strictement supérieur à ω et cofinal à ω est donc $\omega + \omega$. Quant au plus petit cardinal strictement supérieur à ω et cofinal à ω, il faut supposer que l'univers satisfait l'axiome du choix pour pouvoir affirmer que c'est $\aleph_\omega$: cela découle de la question précédente.

16. a) Soit δ la cofinalité de λ. Si $\delta = \lambda$ (autrement dit, si λ est régulier), alors, par le théorème de Cantor, (théorème 4.5), $\lambda^\delta > \lambda$. Sinon, il existe un ordinal limite α tel que $\lambda = \aleph_\alpha$ et $\mathrm{cof}(\alpha) = \mathrm{cof}(\lambda)$, et une application strictement croissante f non strictement majorée de δ dans α (exercice 15, question e)). Pour chaque $\beta \in \delta$, posons $\lambda_\beta = \aleph_{f(\beta)}$ et $\mu_\beta = \lambda$. Pour tout $\beta \in \delta$, on a donc $\lambda_\beta < \mu_\beta$ et, d'après le théorème de König (théorème 4.15) :

$$\mathrm{card}(\bigcup_{\beta\in\delta} \lambda_\beta) = \lambda < \mathrm{card}(\prod_{\beta\in\delta} \mu_\beta) = \lambda^\delta .$$

b) Comme $\aleph_0 = \aleph_0 \times \aleph_0$, on a $2^{\aleph_0} = 2^{\aleph_0 \times \aleph_0} = (2^{\aleph_0})^{\aleph_0}$. De la question précédente, on déduit donc que la cofinalité de $2^{\aleph_0}$ est strictement supérieure à ω.

c) • Supposons que $\mu < \delta \,(\leqslant \lambda)$. Alors, tout élément $f \in \lambda^\mu$ est strictement majoré dans λ (exercice 15, question c)). Cela signifie que λ^μ est inclus dans $\bigcup_{\kappa\in\lambda} \kappa^\mu$.

• Si $\lambda = \mu^+ = 2^\mu$ (λ est donc régulier), alors $\lambda^\mu = (2^\mu)^\mu = 2^{\mu\times\mu} = 2^\mu = \lambda$.

• Sinon, pour tout cardinal κ strictement compris entre μ et λ, on a :

$$\kappa^\mu \leqslant (2^\kappa)^\mu = 2^{\kappa\mu} = 2^\kappa = \kappa^+ \leqslant \lambda ;$$

a fortiori, si $\kappa \leqslant \mu$, on aura $\kappa^\mu \leqslant \lambda$.

Ainsi :
$$\lambda^\mu \leqslant \mathrm{card}(\bigcup_{\kappa\in\lambda} \kappa^\mu) = \sup_{\kappa\in\lambda} \kappa^\mu \leqslant \lambda.$$

L'inégalité $\lambda \leqslant \lambda^\mu$ étant évidente ($\mu \neq 0$), on aboutit bien à $\lambda^\mu = \lambda$.

• Supposons que $\delta \leqslant \mu \leqslant \lambda$. De la question a), et avec HGC, on déduit que :

$2^\lambda = \lambda^+ \leqslant \lambda^\delta \leqslant \lambda^\mu \leqslant \lambda^\lambda = 2^\lambda$. Donc, $\lambda^\mu = 2^\lambda$.

• Supposons que $\lambda < \mu$. Alors, $2^\mu \leqslant \lambda^\mu \leqslant \mu^\mu = 2^\mu$; donc $\lambda^\mu = 2^\mu$.

17. a) On raisonne par l'absurde : soit Φ une fonction strictement croissante (définissable) de On dans On qui n'a pas la propriété annoncée. On désigne par δ le plus petit des ordinaux α tels que $\Phi(\alpha) < \alpha$. On pose $\beta = \Phi(\delta)$: on a $\beta < \delta$, donc, d'après le choix de δ, $\Phi(\beta) \geqslant \beta$. Cela signifie que $\beta < \delta$ et $\Phi(\beta) \geqslant \Phi(\delta)$: Φ n'est pas strictement croissante ; c'est absurde.

b) Soit α un ordinal. On définit, par induction sur les entiers, une famille d'ordinaux $(\alpha_n)_{n\in\omega}$:

• α_0 est n'importe quel ordinal strictement supérieur à α ;

• pour tout $n \in \omega$, $\alpha_{n+1} = \Phi(\alpha_n)$.

On distingue alors deux cas : ou bien il existe un entier n tel que $\alpha_{n+1} = \alpha_n$, et dans ce cas α_n est un point fixe de Φ strictement supérieur à α ; ou bien $n \longmapsto \alpha_n$ est une application strictement croissante non strictement majorée de ω dans l'ordinal limite

$\beta = \sup_{n\in\omega} \alpha_n$; alors β est cofinal à ω, donc Φ est continue en β, ce qui signifie que :

$$\Phi(\beta) = \sup_{\gamma\in\beta} \Phi(\gamma) = \sup_{n\in\omega} \Phi(\alpha_n) \text{ (parce que } \Phi \text{ est croissante) } = \sup_{n\in\omega} \alpha_{n+1} = \beta \,;$$

là encore, on a un point fixe de Φ strictement supérieur à α, à savoir β.

c) Il est clair que les propriétés de croissance stricte et de continuité en un ordinal limite sont préservées par composition. La construction de la question b) peut être refaite avec la fonction $\Psi \circ \Phi$: partant d'un ordinal α quelconque, on prend un ordinal $\alpha_0 > \alpha$, puis, pour chaque $n \in \omega$, on pose $\alpha_{n+1} = (\Psi \circ \Phi)(\alpha_n)$. D'après la question a), on a, pour tout $n \in \omega$, $\alpha_n \leqslant \Phi(\alpha_n) \leqslant (\Psi \circ \Phi)(\alpha_n) = \alpha_{n+1}$. On en déduit que, s'il existe un entier n tel que $\alpha_{n+1} = \alpha_n$, alors α_n est un point fixe commun à Φ et à Ψ, strictement supérieur à α. Dans l'autre éventualité, l'ordinal $\beta = \sup_{n\in\omega} \alpha_n$ est un point fixe de $\Psi \circ \Phi$. Or Φ et Ψ sont strictement croissantes, donc (d'après a)) : $\beta = \Psi \circ \Phi(\beta) \geqslant \Phi(\beta) \geqslant \beta$, et $\beta = \Phi(\beta) = \Psi(\beta)$. On en déduit que β est un point fixe commun à Φ et Ψ, supérieur à α.

d) On applique la question précédente aux fonctions Φ et Ψ qui, à chaque ordinal α, associent respectivement $\aleph_\alpha$ et $\text{card}(V_\alpha)$. Ces fonctions sont continues en tout ordinal limite : cela résulte immédiatement de leurs définitions. La stricte croissance de Φ est également immédiate ; celle de Ψ n'est guère difficile à prouver : si $\alpha < \beta$, alors $\alpha + 1 \leqslant \beta$, donc $\mathfrak{P}(V_\alpha) = V_{\alpha+1} \subseteq V_\beta$, ce qui montre que :

$$\text{card}(V_\alpha) < 2^{\text{card}(V_\alpha)} = \text{card}(V_{\alpha+1}) \leqslant \text{card}(V_\beta).$$

On obtient donc, pour tout ordinal α, un point fixe $\beta > \alpha$, commun à Φ et à Ψ, c'est-à-dire tel que :

$$\aleph_\alpha = \text{card}(V_\alpha) = \alpha.$$

18. a) On utilise les résultats de l'exercice 16. On a $\aleph_\omega = \sup_{n\in\omega} \aleph_n$; mais :

$$\omega^{\aleph_\omega} = 2^{\aleph_\omega} > \aleph_\omega = \sup_{n\in\omega} \aleph_{n+1} = \sup_{n\in\omega} 2^{\aleph_n} = \sup_{n\in\omega} \omega^{\aleph_n}.$$

Donc la première fonction n'est pas continue en ω. La deuxième non plus, d'ailleurs :

$$(\aleph_\omega)^\omega = 2^{\aleph_\omega} > \aleph_\omega = \sup_{n\in\omega} \aleph_{n+1} = \sup_{n\in\omega} (\aleph_{n+1})^\omega.$$

b) Pour la première fonction, la réponse est oui (se reporter à la définition de la somme ordinale). La deuxième fonction n'est pas continue en ω :

$$(\sup_{n\in\omega} n) + \omega = \omega + \omega \,;\text{ tandis que } \sup_{n\in\omega} (n + \omega) = \omega.$$

La troisième fonction est continue en tout ordinal limite : là aussi, il suffit d'examiner la définition du produit ordinal. Enfin, la quatrième fonction n'est pas continue en ω :

$$2.(\sup_{n\in\omega} n) = 2.\omega = \omega + \omega \,;\text{ tandis que } \sup_{n\in\omega} (2.n) = \omega.$$

19. Supposons que l'univers $\mathfrak{U}$ satisfasse AF (il coïncide donc avec la classe $\mathscr{V}$). Si une formule F à une variable libre définit une classe non vide (autrement dit : si $\mathfrak{U} \models \exists v_0 F[v_0]$), alors on peut choisir dans cette classe un élément a de rang minimum (ce

qui signifie qu'il existe un ordinal α tel que $a \in V_\alpha$ et que, pour tout ordinal $\beta < \alpha$, aucun élément de V_β ne satisfasse F). Il est alors clair que pour tout ensemble b tel que $b \in a$, on a $\mathfrak{U} \models \neg F[b]$, puisque le rang de b est strictement inférieur à celui de a. Cela prouve que le schéma d'axiome proposé est satisfait dans $\mathfrak{U}$.

Réciproquement, supposons que ce schéma soit satisfait, et considérons la formule $F[v_0] = \forall v_1(On[v_1] \Rightarrow \neg v_0 \in V_{v_1})$ qui définit la classe $\mathscr{X}$ des ensembles qui ne sont pas dans $\mathscr{V}$. Si la classe $\mathscr{X}$ n'était pas vide, on pourrait trouver, grâce au schéma d'axiome, un ensemble a dans cette classe tel qu'aucun ensemble b appartenant à a ne soit dans la classe $\mathscr{X}$; autrement dit, tous les éléments de a devraient être dans $\mathscr{V}$, c'est-à-dire dans V_α pour un ordinal α approprié ; a serait donc une partie de V_α, c'est-à-dire un élément de $V_{\alpha+1}$, et serait dans la classe $\mathscr{V}$ et non dans la classe $\mathscr{X}$, ce qui serait absurde. La conclusion est que la classe $\mathscr{X}$ est vide, ou encore que l'univers coïncide avec la classe $\mathscr{V}$, ce qui montre qu'il satisfait AF (théorème 5.2).

20. a) Il est clair qu'un ensemble clos cofinal n'est pas vide. Pour montrer que l'ensemble des sous-ensembles clos cofinaux de λ forme une base de filtre, il suffit donc d'appliquer le résultat qui va être montré en b) dans le cas particulier de familles finies d'ensembles clos cofinaux.

b) Posons $X = \bigcap_{i \in I} X_i$. Il est clair que X est clos : si $Y \subseteq X$ et $\text{card } Y < \lambda$, alors, pour tout $i \in I$, $Y \subseteq X_i$, et $\sup Y \in X_i$. Donc $\sup Y \in X$.

Montrons que X est aussi cofinal : soit $a \in \lambda$. On définit par récurrence une suite $(f_n ; n \in \omega)$ d'applications de I dans λ de la façon suivante : pour tout $i \in I$, $f_0(i)$ est le plus petit élément de X_i supérieur à α (il en existe puisque X_i est cofinal) ; pour tout $n \in \omega$ et pour tout $i \in I$, $f_{n+1}(i)$ est le plus petit ordinal de X_i supérieur à $\sup\{f_n(j) ; j \in I\}$. (On remarque que la cardinalité de l'ensemble $\{f_n(j) ; j \in I\}$ est strictement inférieure à λ, et donc $\sup\{f_n(j) ; j \in I\}$ est aussi strictement inférieur à λ.)

Pour tout $i \in I$, $\{f_n(i) ; n \in \omega\}$ est un ensemble dénombrable inclus dans X_i, et donc, $\alpha_i = \sup\{f_n(i) ; n \in \omega\}$ appartient à X_i. Or pour tous i, j appartenant à I, $\alpha_i = \alpha_j$: en effet, par définition des applications f_n, pour tout $n \in \omega$, $f_{n+1}(i) > f_n(j)$, ce qui montre que $\alpha_i \geqslant \alpha_j$. Pour une raison analogue, $\alpha_j \geqslant \alpha_i$, et donc $\alpha_i = \alpha_j$. Par conséquent, la valeur commune de tous les α_i appartient à X.

c) L'implication *1)* $\Rightarrow$ *2)* est à peu près évidente : si Y_1 et Y_2 sont deux ensembles stationnaires disjoints, alors l'un des deux au moins ne contient pas d'ensemble clos cofinal, sinon leur intersection ne serait pas vide.

Les autres implications ne sont pas plus difficiles une fois que l'on a remarqué le fait suivant : soit $\mathscr{F}$ le filtre engendré par les ensembles clos cofinaux ; alors un sous-ensemble Y de λ est stationnaire si et seulement si son complémentaire n'appartient pas à $\mathscr{F}$.

d) On montre d'abord que $\Delta(X)$ est clos : soit Y un sous-ensemble de $\Delta(X)$ dont la cardinalité est strictement inférieure à λ ; Y est bien ordonné par la relation d'appartenance, et donc isomorphe à un ordinal α, qui doit être inférieur à λ : il existe une bijection f strictement croissante de α sur Y. Par définition de $\Delta(X)$, pour tout $\beta \in \alpha$, $f(\beta) \in X_{f(\beta)}$.

Posons $\gamma = \sup Y$. Il s'agit de montrer que $\gamma \in X_\gamma$. Pour tout $\beta \in \alpha$, $\gamma = \sup (f(\delta)\ ;\ \beta \leqslant \delta < \alpha)$. Mais, si $\beta \leqslant \delta < \alpha$, alors $X_{f(\delta)} \subseteq X_{f(\beta)}$ (propriété (2) de l'énoncé), et donc $f(\delta) \in X_{f(\beta)}$. Comme $X_{f(\beta)}$ est un ensemble clos, on en déduit que $\gamma \in X_{f(\beta)}$, et comme ceci est vrai pour tout $\beta \in \alpha$, on voit que $\gamma \in \bigcap_{\beta\in\alpha} X_{f(\beta)}$; or cet ensemble, à cause de la propriété (3) de l'énoncé, est égal à X_γ.

Montrons maintenant que $\Delta(X)$ est cofinal. Soit $\alpha \in \lambda$. On définit alors par récurrence une suite $(\alpha_n\ ;\ n \in \omega)$ par : $\alpha_0 = \alpha$; α_{n+1} est le plus petit ordinal strictement supérieur à α_n appartenant à X_{α_n}. Posons $\beta = \sup(\alpha_n\ ;\ n \in \omega)$. En utilisant toujours le même genre d'argument, on voit que $\beta \in X_\beta$, et donc que $\beta \in \Delta(X)$.

e) On prouve le contraposé du théorème de Fodor : soit f une application de λ dans λ, et on suppose que, pour tout $\alpha \in \lambda$, $f^{-1}(\alpha)$ n'est pas stationnaire. On va construire un ensemble clos cofinal X tel que, pour tout $\alpha \in X$, $f(\alpha) \geqslant \alpha$.

Avec l'axiome du choix et les hypothèses, on trouve une famille $(T_\alpha\ ;\ \alpha \in \lambda)$ de sous-ensembles clos cofinaux de λ, telle que, pour tout $\alpha \in \lambda$, pour tout $\beta \in T_\alpha$, $f(\beta) \neq \alpha$. On définit alors une autre famille $(X_\alpha\ ;\ \alpha \in \lambda)$ de sous-ensembles clos cofinaux de λ, par induction, de la façon suivante :

- $X_0 = \lambda$;
- si α est un ordinal limite, alors $X_\alpha = \bigcap_{\beta\in\alpha} X_\beta$;
- si $\alpha = \beta + 1$, alors $X_\alpha = X_\beta \cap T_\beta$.

La famille $(X_\alpha\ ;\ \alpha \in \lambda)$ satisfait les conditions (1), (2) et (3) de la question précédente, et, de plus, on vérifie sans mal que : pour tout $\alpha \in \lambda$, pour tout $\beta \in X_\alpha$, $f(\beta) \geqslant \alpha$.

Soit Y l'intersection diagonale de cette famille. C'est un ensemble clos cofinal, et si $\alpha \in X$, alors $\alpha \in X_\alpha$, et donc $f(\alpha) \geqslant \alpha$.

f) On va montrer que tout sous-ensemble X clos cofinal de λ contient un ordinal de cofinalité $\aleph_0$. On définit par récurrence une suite d'ordinaux $(\alpha_n\ ;\ n \in \omega)$, strictement croissante, par : α_0 est le plus petit ordinal appartenant à X et α_{n+1} est le plus petit élément de X strictement supérieur à α_n. Il est alors clair que la cofinalité de $\beta = \sup (\alpha_n\ ;\ n \in \omega)$ est $\aleph_0$ et β appartient à X parce que X est clos. Il en résulte donc que l'ensemble des éléments de λ qui sont de cofinalité $\aleph_0$ rencontre tous les clos cofinaux et est donc stationnaire.

On raisonne de même pour montrer que le sous-ensemble de λ composé des ordinaux de cofinalité $\aleph_1$ est stationnaire : si X est un clos cofinal, on définit encore par induction une suite $(\alpha_i\ ;\ i \in \aleph_1)$, strictement croissante, d'éléments de X, et on pose

$\beta = \sup(\alpha_i ; i \in \aleph_1)$; alors $\beta \in X$, et la cofinalité de β est clairement inférieure ou égale à $\aleph_1$. Montrons par l'absurde qu'elle ne peut pas être égale à $\aleph_0$: il existerait une suite strictement croissante d'ordinaux $(\gamma_n ; n \in \omega)$ telle que $\sup(\gamma_n ; n \in \omega) = \beta = \sup(\alpha_i ; i \in \aleph_1)$. Pour chaque entier n, posons :

$$A_n = \{i \in \aleph_1 ; \alpha_i \leqslant \gamma_n\}.$$

Comme la suite $(\alpha_i ; i \in \aleph_1)$ est strictement croissante et n'est pas majorée par γ_n, A_n est un segment initial propre de $\aleph_1$ et est donc dénombrable. Par ailleurs, si $i \in \aleph_1$, il existe un entier n tel que $\alpha_i \leqslant \gamma_n$, ce qui prouve que $\bigcup_{n \in \omega} A_n = \aleph_1$: ce qui est impossible d'après le corollaire 4.14.

Il est bien clair que la cofinalité d'un ordinal ne peut être à la fois $\aleph_0$ et $\aleph_1$: on a bien trouvé deux ensembles stationnaires disjoints.

g) Pour tout $\alpha \in \aleph_1$, $h_n(\alpha) \in \alpha$; on peut donc appliquer le théorème de Fodor : il existe $\beta_n \in \aleph_1$ tel que $h_n^{-1}(\beta_n)$ soit un ensemble stationnaire ; appelons Y_n cet ensemble duquel on a éventuellement ôté 0. Alors, pour tout $\gamma \in Y_n$, $f_\gamma(n) = h_n(\gamma) = \beta_n$.

Soit $\gamma \in \bigcap_{n \in \omega} Y_n$. Pour tout $n \in \omega$, $f_\gamma(n) = h_n(\gamma) = \beta_n$. Comme f_γ est une application surjective de ω sur γ, on voit que $\gamma = \{\beta_n ; n \in \omega\}$. On en déduit donc que $\bigcap_{n \in \omega} Y_n$ n'est pas un ensemble cofinal, donc ne contient aucun ensemble clos cofinal : avec la question b), cela montre que l'un au moins des ensembles Y_n n'appartient pas à $\mathscr{F}$.

21. a) Les remarques faites en 5.4 montrent que, si α est un ordinal limite, alors $\langle V_\alpha, \in \rangle$ satisfait les axiomes d'extentionnalité, de la réunion, de la paire et des parties. D'autre part, parce que α est strictement supérieur à ω, il satisfait aussi l'axiome de l'infini : dans $\langle V_\alpha, \in \rangle$, ω est un ordinal qui n'est ni nul ni successeur.

Restent les axiomes de compréhension. Soient $F[v_0, v_1, \ldots, v_n]$ une formule de $\mathscr{L}$ et b, a_1, $a_2, \ldots, a_n$ des ensembles appartenant à V_α. On sait qu'il existe un ensemble c tel que :

$$\mathfrak{U} \models \forall w(w \in c \Longleftrightarrow (w \in b \wedge F^{V_\alpha}[w, a_1, \ldots, a_n]).$$

Il est bien clair que $c \subseteq b$. Or, il existe $\beta < \alpha$ tel que $b \in V_\beta$, et donc $c \in V_{\beta+1}$. Comme α est un ordinal limite, $\beta + 1 < \alpha$, et $c \in V_\alpha$. Par construction de la formule F^{V_α}, on a :

$\mathfrak{U} \models \forall w(w \in c \Longleftrightarrow (w \in b \wedge F^{V_\alpha}[w, a_1, \ldots, a_n])$ si et seulement si

$$\langle V_\alpha, \in \rangle \models \forall w(w \in c \Longleftrightarrow (w \in b \wedge F[w, a_1, \ldots, a_n]).$$

Les axiomes de compréhension sont bien vrais dans $\langle V_\alpha, \in \rangle$.

b) Si ZF n'est pas consistant, alors ZF n'est certainement pas conséquence de Z qui est consistant par hypothèse. Supposons donc que ZF soit consistant. Il en existe alors un modèle $\mathfrak{U}$. Considérons l'ensemble $V_{\omega+\omega}$ défini à l'intérieur de ce modèle $\mathfrak{U}$. On vient de voir que $\langle V_{\omega+\omega}, \in \rangle$ est un modèle de Z. Ce n'est pas un modèle de ZF : sinon on pourrait définir par induction une suite d'ordinaux $(\alpha_n ; n \in \omega)$, par :

$\alpha_0 = \omega$;

$\alpha_{n+1} = \alpha_n + 1$.

On voit alors que, dans $< V_{\omega+\omega}, \in >$, $\bigcup_{n\in\omega} \alpha_n$ est un ensemble qui est égal à la classe de tous les ordinaux, ce qui contredit la proposition 1 de 2.6.

22 Tout d'abord, $<\mathscr{W}, \in>$ satisfait l'axiome d'extensionnalité : celui-ci est une formule universelle et $<\mathscr{W}, \in>$ est une sous-structure de $\mathfrak{U}$. D'autre part, pour tous ensembles x et y, $cl(\{x,y\}) = cl(x) \cup cl(y) \cup \{x,y\}$, et donc $cl(\{x,y\})$ est dénombrable si $cl(x)$ et $cl(y)$ le sont. Il en résulte que $<\mathscr{W}, \in>$ satisfait l'axiome de la paire. Par définition même de la clôture transitive, pour tout ensemble x, $cl(\bigcup_{t\in x} t) \subseteq cl(x)$, ce qui montre que $<\mathscr{W}, \in>$ satisfait l'axiome de la réunion.

On laisse aussi le lecteur vérifier, en se reportant à la définition des ordinaux, que, pour tout x dans $\mathscr{W}$:

$$<\mathscr{W}, \in> \models On(x) \quad \text{si et seulement si} \quad \mathfrak{U} \models On(x).$$

Or $cl(\omega) = \omega$, et donc ω est dans $\mathscr{W}$ et on voit que :

$<\mathscr{W}, \in> \models$ « ω est un ordinal qui n'est ni vide ni successeur ».

Par conséquent $<\mathscr{W}, \in>$ satisfait l'axiome de l'infini.

Il reste le plus difficile, c'est-à-dire les axiomes de remplacement. Notons $W[v_0]$ la formule : « $cl(v_0)$ est dénombrable ». Soient $F[w_0,w_1,v_0,v_1,\ldots,v_n]$ une formule de $\mathscr{L}$, b, a_0, a_1, ...,a_n des ensembles se trouvant dans $\mathscr{W}$, et on suppose que la formule $F[w_0,w_1,a_0,a_1,\ldots,a_n]$ est fonctionnelle en w_0 dans $<\mathscr{W}, \in>$, c'est-à-dire que :

$$<\mathscr{W}, \in> \models \forall w_0 \forall w_1 \forall w_2((F[w_0,w_1,a_0,a_1,\ldots,a_n] \wedge F[w_0,w_2,a_0,a_1,\ldots,a_n]) \Longrightarrow w_1 \simeq w_2).$$

Cela implique :

$$\mathfrak{U} \models \forall w_0 \forall w_1 \forall w_2((W[w_0] \wedge W[w_1] \wedge W[w_2] \wedge F^{\mathscr{W}}[w_0,w_1,a_0,a_1,\ldots,a_n] \wedge F^{\mathscr{W}}[w_0,w_2,a_0,a_1,\ldots,a_n]) \Longrightarrow w_1 \simeq w_2),$$

et donc, la formule $W[w_0] \wedge W[w_1] \wedge F^{\mathscr{W}}[w_0,w_1,a_0,a_1,\ldots,a_n]$ est fonctionnelle en w_0 dans $\mathfrak{U}$. Par remplacement dans $\mathfrak{U}$, on en déduit qu'il existe un ensemble c tel que :

(*) $\mathfrak{U} \models \forall v_0(v_0 \in c \Longleftrightarrow \exists w_0 \in b\ (W[w_0] \wedge W[v_0] \wedge F^{\mathscr{W}}[w_0,v_0,a_0,a_1,\ldots,a_n])$.

L'ensemble c est dénombrable (la formule $F^{\mathscr{W}}[w_0,w_1,a_0,a_1,\ldots,a_n]$ définit une application surjective d'une partie de b, qui est dénombrable parce qu'il est dans $\mathscr{W}$, sur c (proposition 4.9)). Par ailleurs, tous les éléments de c sont dans $\mathscr{W}$ (par définition). Comme $cl(c) = c \cup \bigcup_{t\in c} cl(t)$, on voit que c est dans $\mathscr{W}$. De la relation (*), on déduit :

$$<\mathscr{W}, \in> \models \forall v_0(v_0 \in c \Longleftrightarrow \exists w_0 \in b\ (F[w_0,v_0,a_0,a_1,\ldots,a_n]).$$

Les axiomes de remplacement sont donc vérifiés dans $<\mathscr{W}, \in>$.

Il est bien clair que toutes les parties de ω sont dans $\mathscr{W}$, mais que $\mathfrak{P}(\omega)$, qui n'est pas dénombrable, n'est pas dans $\mathscr{W}$: cela montre que $<\mathscr{W}, \in>$ ne satisfait pas l'axiome des parties.

23. Chaque nombre réel r de l'intervalle]0,1] admet un développement décimal. Cela veut dire qu'il existe une suite $(a_i\ ;\ i \in \omega)$ de nombres entiers compris, au sens large, entre 0 et 9 telle que :

$$r = \sum_{i \geqslant 1} \frac{a_i}{10^i}$$

Il n'y a pas unicité. Cependant, si on pose :

$S^* = \{ s \in \{0,1,2,3,4,5,6,7,8,9\}^\omega$; pour tout $n \in \omega$, il existe $p \geqslant n$ tel que $s(p) \neq 0 \}$,

alors, pour tout $r \in]0,1]$, il existe un et un seul élément $(a_i\ ;\ i \in \omega)$ de S^* tel que $r = \sum_{i \geqslant 1} \frac{a_i}{10^i}$.

Pour montrer que l'intervalle]0,1] n'est pas dénombrable, il suffit donc de montrer que S^* ne l'est pas, ou, ce qui revient au même que si $(s^i\ ;\ i \in \omega)$ est une suite d'éléments de S^*, alors il existe un élément s dans S^* qui n'est égal à aucun des s^i. Il suffit de définir la suite s par :

$s(i) = 1$ si $s^i(i) \neq 1$;

$s(i) = 2$ si $s^i(i) = 1$.

CHAPITRE 8

1. a) On peut tout d'abord remarquer que l'ensemble $\mathbb{N}^* = \mathbb{N} - \{0\}$ est un exemple d'ensemble disjoint de l'ensemble de ses parties (0 appartient à tous les éléments de $\mathbb{N}^*$ mais à aucune de ses parties).

$\mathfrak{M}_X \models H_0$ parce que X et $\mathfrak{P}(X)$ constituent une partition de M_X ; $\mathfrak{M}_X \models H_1$ parce que, pour tout couple $(x,y) \in \overline{A}$, on a $x \in X$ et $y \in \mathfrak{P}(X)$; $\mathfrak{M}_X \models H_2$ par extensionnalité ; $\mathfrak{M}_X \models H_3$ parce que l'ensemble vide est un élément de $\mathfrak{P}(X)$; $\mathfrak{M}_X \models H_4$ parce que toute partie $x \in \mathfrak{P}(X)$ a un complémentaire dans X ; $\mathfrak{M}_X \models H_5$ parce que, pour toute parties $x \in \mathfrak{P}(X)$ et $y \in \mathfrak{P}(X)$, $x \cup y \in \mathfrak{P}(X)$; enfin, pour chaque entier $n \geqslant 1$, $\mathfrak{M}_X \models F_n$ parce que, quels que soient les éléments $x_1, x_2, ..., x_n$ de X, $\{x_1,x_2,...,x_n\} \in \mathfrak{P}(X)$.

b) Oui : le langage est dénombrable, la théorie T admet des modèles infinis (par exemple, le modèle $\mathfrak{M}_X$ de la question a), en choisissant X infini), donc (théorème de Lowenheim-Skolem descendant, 1.5) T admet un modèle dénombrable ; on peut d'ailleurs aisément en décrire un en s'inspirant de la question a) avec un ensemble X dénombrable : c'est la sous-structure de $\mathfrak{M}_X$ dont l'ensemble de base est $X \cup \mathfrak{P}_f(X) \cup \mathfrak{P}_{cof}(X)$, où $\mathfrak{P}_f(X)$ est l'ensemble des parties finies de X et $\mathfrak{P}_{cof}(\mathbb{N})$ est l'ensemble des parties cofinies de X. Il est facile de vérifier qu'il s'agit d'un modèle dénombrable de T.

c) Ce sont les entiers de la forme $k + 2^k$, où $k \in \mathbb{N}$.

d) On laisse au lecteur le soin de montrer par récurrence, en se servant de H_5, que, pour tout entier $n \geqslant 1$, on a : $\{H_0,H_1,H_2,H_3,H_4,H_5,F_1\} \vdash F_n$.

e) Désignons par $\mathfrak{M}_0$ le modèle dénombrable de T décrit à question b), dont l'ensemble de base est $X \cup \mathfrak{P}_f(X) \cup \mathfrak{P}_{cof}(X)$ (pour fixer les idées, on va prendre $X = \mathbb{N}^*$). Nous allons décrire un modèle dénombrable $\mathfrak{M}_1$ de T, non isomorphe à $\mathfrak{M}_0$. Soit C un sous-ensemble infini et de complémentaire infini de X (l'ensemble des entiers strictement positifs pairs par exemple). Considérons la sous-algèbre de Boole de $\mathfrak{P}(X)$ engendrée par $\mathfrak{P}_f(X) \cup \mathfrak{P}_{cof}(X) \cup \{C\}$; on obtient ainsi une sous-algèbre de Boole B de $\mathfrak{P}(X)$ qui est encore dénombrable. On prend alors pour structure $\mathfrak{M}_1$ la sous-structure de $\mathfrak{M}_X$ dont l'ensemble de base est $X \cup B$, et il est facile de vérifier que c'est un modèle de T.

Nous allons maintenant montrer que $\mathfrak{M}_0$ n'est pas isomorphe à $\mathfrak{M}_1$. Pour chaque entier $p > 0$, considérons la formule $F_p[v_0]$:

$$\exists v_1 \exists v_2 ... \exists v_p (\forall w_0 (A w_0 v_0 \Rightarrow (\bigvee_{1 \leqslant i \leqslant p} w_0 \simeq v_i))).$$

Alors $\mathfrak{M}_0$ possède la propriété suivante : pour tout élément x de $\mathfrak{M}_0$, il existe un entier p tel que $\mathfrak{M}_0 \models F_p[x]$.

Evidemment cette propriété est encore satisfaite par toute structure isomorphe à $\mathfrak{M}_0$; or elle ne l'est pas par $\mathfrak{M}_1$, car C ne satisfait aucune des formules F_p dans $\mathfrak{M}_1$.

2. Les préliminaires auxquels on se référera dans ce qui suit sont ceux du corrigé de l'exercice 15 du chapitre 3.

a) • Il est clair que la relation $\approx$ est réflexive (prendre $m = n = p = q = 0$ dans la définition) et symétrique. Supposons que a, b, $c \in M$, $a \approx b$ et $b \approx c$. Il y a alors des entiers naturels m, n, p, q, r, s, t et u tels que :

$$\bar{d}^m(\bar{g}^n(a)) = \bar{d}^p(\bar{g}^q(b)) \text{ et } \bar{d}^r(\bar{g}^s(b)) = \bar{d}^t(\bar{g}^u(c)).$$

Le fait que $\bar{d}$ et $\bar{g}$ commutent entraîne (voir préliminaires) :

$$\bar{d}^{m+r}(\bar{g}^{n+s}(a)) = \bar{d}^{p+r}(\bar{g}^{q+s}(b)) = \bar{d}^{t+p}(\bar{g}^{u+q}(c)),$$

ce qui prouve $a \approx c$.

• Comme, pour tout élément a de M, $a \approx \bar{d}(a)$ et $a \approx \bar{g}(a)$, la grille de a est stable par les applications $\bar{d}$ et $\bar{g}$.

On notera que cette propriété est plus forte que la compatibilité de la relation $\approx$ avec les applications $\bar{d}$ et $\bar{g}$ (qui s'énonce, elle : si $a \approx b$, alors $\bar{d}(a) \approx \bar{d}(b)$ et $\bar{g}(a) \approx \bar{g}(b)$).

• Soit G une grille de $\mathfrak{M}$. La stabilité de G par $\bar{d}$ et $\bar{g}$ est suffisante pour que $\langle G, \bar{d}\restriction_G, \bar{g}\restriction_G \rangle$ constitue une sous-structure $\mathfrak{G}$ de $\mathfrak{M}$. Toutes les formules closes universelles de L satisfaites dans $\mathfrak{M}$ sont également satisfaites dans $\mathfrak{G}$ (corollaire 5.3). Pour montrer que $\mathfrak{G}$ est un modèle de T, il suffit donc de s'assurer que $\mathfrak{G}$ satisfait les seules formules de T qui ne soient pas universelles, c'est-à-dire les formules $\forall x \exists u\, du \simeq x$ et $\forall x \exists v\, gv \simeq x$. Soit donc a un élément de G. Comme ces formules sont vraies dans $\mathfrak{M}$, on peut trouver dans M deux éléments b et c tels que $a = \bar{d}(b) = \bar{g}(c)$. Mais on vient de démontrer que $\bar{d}(b) \approx b$ et $\bar{g}(c) \approx c$. Il en résulte que b et c sont dans la même grille que a, c'est-à-dire dans G, ce qui prouve que les formules considérées sont satisfaites dans $\mathfrak{G}$.

• Le modèle standard (voir corrigé de l'exercice 15 du chapitre 3) admet une unique grille : considérons en effet deux couples (i,j) et (k,l) d'entiers relatifs et posons $m = \sup(l-j, 0)$, $n = \sup(k-i, 0)$, $p = \sup(j-l, 0)$ et $q = \sup(i-k, 0)$; il est facile de vérifier qu'on a alors :

$$s_d{}^m(s_g{}^n(i,j)) = s_d{}^p(s_g{}^q(k,l)),$$

ce qui montre que $(i,j) \approx (k,l)$.

Montrons maintenant une propriété qui nous sera utile dans les questions suivantes : dans un modèle $\mathfrak{M} = \langle M, \bar{d}, \bar{g} \rangle$ de T, toute grille G définit une L-structure $\mathfrak{G} = \langle G, \bar{d}\restriction_G, \bar{g}\restriction_G \rangle$ isomorphe à la structure standard $\mathfrak{M}_0$.

Soit a un élément de G. On considère alors l'application φ de $\mathbb{Z} \times \mathbb{Z}$ dans M qui, à chaque couple (i,j) d'entiers relatifs, associe l'élément $\bar{d}^j(\bar{g}^i(a))$ de M. On laisse alors au lecteur le soin de vérifier que φ est injective, que son image est G, et que φ est un isomorphisme de $\mathfrak{M}_0$ dans $\mathfrak{G}$.

qui est un modèle de T', la L-structure sous-jacente $\mathfrak{M} = <M, \overline{d}, \overline{g}>$ est évidemment un modèle de T, et les éléments $\overline{\lambda}$ et $\overline{\mu}$ ne sont pas ≈-équivalents, car, s'ils l'étaient, l'une des formules G_{mnpq} ne serait pas satisfaite dans $\mathfrak{M}'$. Le modèle $\mathfrak{M}$ contient donc au moins deux grilles distinctes (celle de $\overline{\lambda}$ et celle de $\overline{\mu}$) et n'est donc pas isomorphe au modèle standard. L'existence d'un modèle pour la théorie T' implique donc l'existence d'un modèle non standard pour la théorie T.

Il ne nous reste plus qu'à montrer l'existence d'un modèle pour T', ce qui revient, en vertu du théorème de compacité, à montrer l'existence d'un modèle pour chaque partie finie de T'. Soit donc T_0 une partie finie de T'. Il existe un entier naturel N tel que : $T_0 \subseteq T_N = T \cup \{G_{mnpq} ; \sup(m,n,p,q) \leqslant N\}$. Appelons $\mathfrak{M}_N$ la L'-structure obtenue en enrichissant la L-structure standard $\mathfrak{M}_0$ des interprétations suivantes pour λ et μ :

$$\overline{\lambda} = (0,0) , \overline{\mu} = (N+1, N+1).$$

Si m, n, p et q sont des entiers naturels inférieurs ou égaux à N, on a $s_d{}^m(s_g{}^n(\overline{\lambda})) = (n, m)$ alors que $s_d{}^p(s_g{}^q(\overline{\mu})) = (N+q+1, N+p+1)$, ce qui montre que la formule G_{mnpq} est satisfaite dans la structure $\mathfrak{M}_N$ qui est, de ce fait, un modèle de T_N, et à fortiori de T_0.

c) On considère la structure $\mathfrak{M}_A = <M_A, d_A, g_A>$, où :

- $M_A = A \times \mathbb{Z} \times \mathbb{Z}$;
- pour tout $a \in A$, pour tous i, j $\in \mathbb{N}$, $d_A((a,i,j)) = (a,i+1,j)$ et $d_B((a,i,j)) = (a,i,j+1)$.

On vérifie sans peine que $\mathfrak{M}_A$ est un modèle de T ; par ailleurs si (a,i,j) et (a',i',j') sont des éléments de M_A, alors (a,i,j) ≈ (a',i',j') si et seulement si a = a' : l'application qui à $a \in A$ fait correspondre l'ensemble $\{(a,i,j) ; (i,j) \in \mathbb{Z} \times \mathbb{Z}\}$ est une bijection de A sur l'ensembles des grilles de $\mathfrak{M}_A$.

On peut naturellement considérer que cette question rend la précédente superflue, puisqu'on a ici fait plus que montrer l'existence de modèles non standard de T : on en a explicitement décrits.

d) Soient $\mathfrak{M} = <M, d_1, g_1>$ et $\mathfrak{N} = <N, d_2, g_2>$ deux modèles de T et σ une bijection de l'ensemble M/≈ des grilles de $\mathfrak{M}$ sur l'ensemble N/≈ des grilles de $\mathfrak{N}$. Comme on a vu que toute grille est isomorphe au modèle standard, on en déduit qu'entre deux grilles quelconques (pas nécessairement extraites d'un même modèle) on peut toujours trouver au moins un isomorphisme. Pour chaque grille $G \in M/\approx$, choisissons un isomorphisme φ_G de G sur $\sigma(G)$ (remarquer qu'on confond une grille et la L-structure qui lui a été associée, et remarquer d'autre part qu'on utilise l'axiome du choix).

La réunion φ de toutes les applications φ_G, pour $G \in M/\approx$, est un isomorphisme de $\mathfrak{M}$ sur $\mathfrak{N}$.

e) Si on prend pour A un ensemble à un élément et pour B un ensemble à deux éléments, on voit que les modèles $\mathfrak{M}_A$ et $\mathfrak{M}_B$,qui sont dénombrables, ne sont pas isomorphes : $\mathfrak{M}_A$ n'a qu'une seule grille, $\mathfrak{M}_B$ en a deux. Donc T n'est pas $\aleph_0$-catégorique.

D'autre part, si $\mathfrak{M}$ est un modèle de T et si on appelle C l'ensemble de ses grilles, on voit, d'après la question d), que $\mathfrak{M}$ est isomorphe à $\mathfrak{M}_C$, et donc que :

$$\text{card}(M) = \text{card}(C \times \mathbb{Z} \times \mathbb{Z}) = \sup(\aleph_0, \text{card}(C)).$$

Il en résulte que le cardinal de l'ensemble des grilles d'un modèle dénombrable de T est, soit un entier strictement positif, soit $\aleph_0$; c'est donc un élément non nul de l'ensemble dénombrable $\omega + 1 = \omega \cup \{\omega\}$.

L'application c de $\mathscr{X}$ dans $\omega + 1$ qui à chaque élément de $\mathscr{X}$ associe le cardinal de son ensemble de grilles est injective : en effet, si $\mathfrak{M} \in \mathscr{X}$, $\mathfrak{N} \in \mathscr{X}$ et $c(\mathfrak{M}) = c(\mathfrak{N})$, alors, d'après la question d), $\mathfrak{M}$ et $\mathfrak{N}$ sont isomorphes, et d'après les propriétés de $\mathscr{X}$, $\mathfrak{M} = \mathfrak{N}$. Cela prouve que le cardinal de $\mathscr{X}$ est au plus $\aleph_0$.

Mais, on a vu que, pour tout élément x non nul de $\omega + 1$, $\mathfrak{M}_x$ est un modèle de T dont l'ensemble de grilles a pour cardinal x. Les propriétés de $\mathscr{X}$ montrent qu'on peut y trouver un modèle isomorphe à $\mathfrak{M}_x$. L'application c est donc surjective sur $(\omega + 1) - \{0\}$.

Le cardinal de $\mathscr{X}$ est donc exactement $\aleph_0$.

f) Soit κ un cardinal non dénombrable. On a vu que, si $\mathfrak{M}$ est un modèle de T et si C est l'ensemble de ses grilles, alors $\text{card}(M) = \sup(\aleph_0, \text{card}(C))$. Cela implque que si la cardinalité de M est égale à κ non dénombrable, la cardinalité de C est aussi égale à κ. Donc, tous les modèles de cardinalité κ sont isomorphes : T est catégorique en tout cardinal non dénombrable.

3. On raisonne par induction sur t. Si t est une variable x, alors :

$$T \vdash \forall x\, t \simeq f_e x.$$

Si $t = f_\beta u$, et si on suppose (hypothèse d'induction) que $T \vdash \forall x\, u \simeq f_\alpha x$, alors on a : $T \vdash \forall x\, t \simeq f_\beta f_\alpha x$, donc, d'après le deuxième ensemble de formules de T si on pose $\gamma = \beta\alpha$:

$$T \vdash \forall x\, t \simeq f_\gamma x.$$

Ce raisonnement montre aussi qu'on peut prendre pour la variable x celle qui apparaît dans le terme t (il y en a une et une seule, puisqu'il n'y a que des symboles de fonction unaires, et pas de symboles de constante).

b) En l'absence de symbole de relation autre que le symbole d'égalité, toute formule atomique s'écrit $t \simeq u$, t et u étant des termes. Puisque chaque terme comporte exactement une variable, chaque formule atomique comporte au plus deux variables.

Etant donnée une formule atomique $F[v_0,v_1]$, il existe donc deux termes t et u tels que $F = t \simeq u$. On peut toujours supposer que v_0 est la variable qui apparaît en t, et, en appelant x la variable de u, on a : $x = v_0$ ou $x = v_1$. Comme on l'a vu en a), il existe des éléments β et γ de G tels que :

$T \vdash \forall v_0\, t \simeq f_\beta v_0$ et $T \vdash \forall x\, u \simeq f_\gamma x$.

Posons $\alpha = \beta^{-1} \circ \gamma$.

• Si $x = v_0$, on a :

$$T \vdash \forall v_0(F \Longleftrightarrow f_\beta v_0 \simeq f_\gamma v_0) ;$$

et donc,

$$T \vdash \forall v_0(F \Longleftrightarrow v_0 \simeq f_\alpha v_0) ;$$

si $\alpha = e$, on obtient $T \vdash \forall v_0 \forall v_1 F$, et si $\alpha \neq e$ $T \vdash \forall v_0 \forall v_1 \neg F$.

• Si $x = v_1$, on a :

$$T \vdash \forall v_0 \forall v_1(F \Longleftrightarrow f_\beta v_0 \simeq f_\gamma v_1) ;$$

donc :

$$T \vdash \forall v_0 \forall v_1(F \Longleftrightarrow v_0 \simeq f_\alpha v_1).$$

c) La vérification ne pose pas de problème et est laissée au lecteur.

d) Pour montrer que $O(a)$ est une sous-structure de $\mathfrak{M}$, on utilise le fait que, pour tous α, β dans G, $\varphi_\beta(\varphi_\alpha(a)) = \varphi_{\beta \cdot \alpha}(a)$. On vérifie sans problème que l'application qui à α fait correspondre $\varphi_\alpha(a)$ est un monomorphisme de $\mathfrak{G}$ dans $\mathfrak{M}$, et que son image est $O(a)$.

Montrons que X_M est une partition de M. On remarque d'abord que si $b \in O(a)$, alors $a \in O(b)$ (si $b = \varphi_\alpha(a)$, alors $a = \varphi_{\alpha^{-1}}(b)$), et $O(a) = O(b)$. Supposons que $O(a)$ et $O(b)$ ne soient pas disjoints ; alors, si c appartient à leur intersection, $O(a) = O(c) = O(b)$. Deux éléments distincts de X_M sont donc disjoints, et, par ailleurs, il est bien clair que la réunion des éléments de X_M est M tout entier.

On va maintenant supposer que les partitions X_M et X_N, correspondantes à deux modèles $\mathfrak{M}$ et $\mathfrak{N}$ sont équipotentes. Grâce à l'axiome du choix, on peut trouver deux familles, $(a_x ; x \in X_M)$ et $(b_y ; y \in X_N)$, telles que, pour tout $x \in X_M$, $a_x \in x$ et pour tout $y \in X_N$, $a_y \in y$. Il existe une bijection σ de X_M sur X_N, et l'application τ de $\{a_x ; x \in X_M\}$ sur $\{b_y ; y \in X_N\}$ définie par : pour tout $x \in X_M$, $\tau(a_x) = b_{\sigma(x)}$ est bijective. Le lecteur vérifiera alors que l'application π définie par :

$$\text{pour tout } \alpha \in G, \text{ pour tout } x \in X_M,\ \pi(\varphi_\alpha(a_x)) = \varphi_\alpha(\tau(a_x))$$

est un isomorphisme de $\mathfrak{M}$ sur $\mathfrak{N}$.

e) Par une démonstration analogue à celle du f) de l'exercice 2, on montre que si κ est un cardinal infini strictement supérieur à celui de G, alors T est κ catégorique. Tout modèle de T contient une copie de G, et est donc infini : T est complète par le théorème de Vaught.

f) Si le cardinal κ de G est fini, le raisonnement qui précède est encore valable pour tous les modèles de cardinal λ infini : la théorie T est λ-catégorique ; toutefois, on ne peut plus conclure que la théorie est complète, car, cette fois, elle a des modèles finis, en particulier le modèle $\mathfrak{G}$, et le théorème de Vaught ne peut pas être appliqué ; la formule :

$$\exists x_1 \exists x_2 \ldots \exists x_\kappa \Big(\bigwedge_{1 \leqslant i < j \leqslant \kappa} \neg x_i \simeq x_j \ \wedge\ \forall x \bigvee_{1 \leqslant i \leqslant \kappa} x \simeq x_i \Big)$$

est satisfaite dans le modèle $\mathfrak{G}$ mais n'est pas satisfaite dans un modèle infini de T (tel

que celui qu'on obtiendrait en prenant la réunion d'une infinité dénombrable de copies de $\mathfrak{G}$ deux à deux disjointes). La théorie T n'est donc pas complète dans ce cas. Cependant, on obtient une théorie complète en ajoutant à T les formules exprimant que l'ensemble de base est infini (voir 5.6, chapitre 3) : on est alors à nouveau dans les conditions d'application du théorème de Vaught.

4. a) Pour $k \in \mathbb{N} - \{0,1\}$, on note respectivement F_k et G_k les formules :

$$\exists v_1 \exists v_2 \ldots \exists v_k \bigwedge_{1 \leq i < j \leq k} \neg R v_i v_j \ ;$$

et

$$\forall v_0 \exists v_1 \exists v_2 \ldots \exists v_k \Big(\bigwedge_{1 \leq i < j \leq k} \neg v_i \simeq v_j \wedge \bigwedge_{1 \leq i \leq k} R v_0 v_i \Big).$$

On pose par ailleurs :

$$EQ = \{ \forall v_0 R v_0 v_0 \ ; \ \forall v_0 \forall v_1 (R v_0 v_1 \Longrightarrow R v_1 v_0) \ ; \ \forall v_0 \forall v_1 \forall v_2 ((R v_0 v_1 \wedge R v_1 v_2) \Longrightarrow R v_0 v_2) \}.$$

On peut prendre pour théorie T :

$$T = EQ \cup \{ F_k \ ; \ k \in \mathbb{N} - \{0,1\} \} \cup \{ G_k \ ; \ k \in \mathbb{N} - \{0,1\} \}.$$

(Le premier de ces ensembles exprime le fait que l'interprétation de R est une relation d'équivalence, le deuxième qu'elle admet une infinité de classes d'équivalence, et le troisième que chacune de ces classes est infinie.)

Soient A et B deux ensembles non vides. On considère la L-structure $\mathfrak{M}_{A,B} = \langle M_{A,B}, R_{A,B} \rangle$ définie par : $M_{A,B} = A \times B$ et pour tous (a,b), (a',b') appartenant à $M_{A,B}$, $R_{A,B}((a,b),(a',b'))$ si et seulement si $a = a'$. C'est un modèle de EQ, et si A et B sont tous les deux infinis, c'est un modèle de T.

b) Supposons que T soit équivalente à un ensemble fini A de formules. Par compacité, chacune des formules de A est conséquence d'un sous-ensemble fini de T, et donc, A lui-même est conséquence d'un sous-ensemble fini S de T. Comme T est conséquence de A, T est conséquence de S, et T et S sont équivalentes. On peut trouver un entier N tel que S soit inclus dans

$$T_N = EQ \cup \{ F_k \ ; \ 1 < k < N \} \cup \{ G_k \ ; \ 1 < k < N \}.$$

On obtient un contradiction en considérant des ensembles A et B de cardinalité N : $\mathfrak{M}_{A,B}$ est un modèle de T_N mais pas de T.

c) Soit λ un cardinal infini non dénombrable. Alors les structures $\mathfrak{M}_{\lambda,\omega}$ et $\mathfrak{M}_{\omega,\lambda}$ sont deux modèles de T de cardinalité λ qui ne sont pas isomorphes : chaque classe de la première est dénombrable, tandis que les classes de la seconde sont de cardinalité λ : La théorie T n'est donc catégorique en aucun cardinal infini non dénombrable. On voit de plus que si $\mathfrak{M}'$ est un modèle de T et s'il existe une injection de $\mathfrak{M}_{\lambda,\omega}$ dans $\mathfrak{M}'$, alors $\mathfrak{M}'$ a au moins λ classes : il ne peut donc pas exister d'injection élémentaire de $\mathfrak{M}_{\lambda,\omega}$ dans $\mathfrak{M}_{\omega,\lambda}$. De même s'il existe une injection de $\mathfrak{M}_{\omega,\lambda}$ dans $\mathfrak{M}'$, alors certaines classes de $\mathfrak{M}'$ (celles contenant l'image d'un élément de $\mathfrak{M}_{\omega,\lambda}$) sont de cardinalité au moins λ, et il n'y a donc pas d'injection élémentaire de $\mathfrak{M}_{\omega,\lambda}$ dans $\mathfrak{M}_{\lambda,\omega}$.

Soient $<M, R_M>$ et $<N, R_N>$ deux modèles dénombrables de T. Les ensembles M/R_M et N/R_N étant infinis, donc dénombrables, on peut choisir une bijection $\varphi : M/R_M \longmapsto N/R_N$. Les classes d'équivalence pour R_M et pour R_N sont également dénombrables ; on peut donc pour chaque $i \in M/R_M$, trouver une bijection f_i de i sur $\varphi(i)$.

La réunion des f_i, c'est-à-dire l'application $f : M \longmapsto N$, définie par :

$$\text{pour tout } a \in M, \quad f(a) = f_{cl(a)}(a),$$

($cl(a)$ étant la classe de a modulo R_M), est une bijection de M dans N et c'est un isomorphisme de $<M, R_M>$ sur $<N, R_N>$.

Ainsi, la théorie T est $\aleph_0$-catégorique, et n'est catégorique en aucun cardinal infini autre que $\aleph_0$.

d) Ce qui vient d'être dit permet de conclure, avec le théorème de Vaught, que T est une théorie complète, après avoir remarqué qu'elle n'admet que des modèles infinis (ce qui est évident).

e) Toute L-structure qui est un modèle de T peut être enrichie en une L_∞-structure qui est un modèle de T_+ : il suffit d'interpréter les symboles c_n, pour $n \in \mathbb{N}$, par des éléments se trouvant dans des classes différentes (ce qui est possible puisqu'il y a une infinité de telles classes). Par exemple, si on part du modèle $\mathfrak{M}_{A,B}$ construit à la question a), avec A et B infinis, on peut choisir des points a_n, pour $n \in \mathbb{N}$, de A, deux à deux distincts, et un point b de B : on peut alors interpréter c_n par (a_n, b), et on obtient ainsi un modèle de T_+.

Pour montrer que T_+ n'est pas équivalente à une théorie finie, on montre que toute partie finie de T_+ admet un modèle fini ; on utilise pour cela un argument analogue à celui qui nous a servi a la question b).

f) Le raisonnement utilisé à la question c) pour montrer que la théorie T n'est catégorique en aucun cardinal infini non dénombrable peut être repris pour aboutir à la même conclusion au sujet de la théorie T_+ : il suffit d'enrichir les deux modèles non isomorphes de cardinalité λ qui y avaient été construits en des modèles de T_+, de la manière indiquée au début de la question e) ; les L_∞-structures ainsi obtenues ne peuvent pas être isomorphes.

Mais, à la différence de T, la théorie T_+ n'est pas $\aleph_0$-catégorique. En effet, prenons le modèle $\mathfrak{M}_{\mathbb{N},\mathbb{N}}$ de la question a) et enrichissons-le en une L_∞-structure de deux façon différentes : d'une part en interprétant, pour chaque $n \in \mathbb{N}$, le symbole c_n par l'entier n ; on obtient ainsi un modèle dénombrable de T_+ que l'on va appeler $\mathfrak{M}_0$; d'autre part, en interprétant, pour chaque $n \in \mathbb{N}$, le symbole c_n par l'entier $n + 1$; soit $\mathfrak{M}_1$ le modèle ainsi obtenu. Ces modèles ne peuvent pas être isomorphes pour la raison suivante : tout monomorphisme h de $\mathfrak{M}_0$ dans $\mathfrak{M}_1$ devra envoyer n sur $n + 1$, et donc, pour tout $n \in \mathbb{N}$, l'ensemble $\{x \in \mathbb{N} \times \mathbb{N} ; \mathfrak{M}_0 \models R(c_n, x)\} = \{(n, y) ; y \in \mathbb{N}\}$ dans l'ensemble $\{x \in \mathbb{N} \times \mathbb{N} ; \mathfrak{M}_1 \models R(c_n, x)\} = \{(n + 1, y) ; y \in \mathbb{N}\}$. Le point $(0,0)$ n'appartient pas à l'image de h ; il n'y a donc pas de monomorphisme surjectif de $\mathfrak{M}_0$ sur $\mathfrak{M}_1$.

g) Soient R_1 et R_2 les interprétations de R dans $\mathfrak{M}_1$ et $\mathfrak{M}_2$ respectivement, et, pour tout $p \in \mathbb{N}$, a_p et b_p les interprétations de c_p dans $\mathfrak{M}_1$ et $\mathfrak{M}_2$ respectivement. On définit d'abord une bijection h de M_1/R_1 sur M_2/R_2 de sorte que, pour tout entier p, si $0 \leqslant p \leqslant n$, $h(cl(a_p)) = cl(b_p)$ ($cl(x)$ désigne la classe de x modulo R_1 ou R_2 suivant le cas) (c'est évidemment possible) ; puis, pour chaque $\alpha \in M_1/R_1$, on définit une bijection f_α de α sur $h(\alpha)$; on exige de plus que si $\alpha = cl(a_p)$ (avec $0 \leqslant p \leqslant n$) alors $f_\alpha(a_p) = b_p$. La réunion des applications f_α, pour $\alpha \in M_1/R_1$, est un isomorphisme de $\mathfrak{M}_1 \upharpoonright L_n$ sur $\mathfrak{M}_2 \upharpoonright L_n$.

On peut maintenant montrer par l'absurde que T_+ est une théorie complète dans L_∞ : si elle ne l'était pas, on pourrait trouver une formule close F de L_∞, un modèle dénombrable $\mathfrak{M}_1$ de $T \cup \{F\}$ et un modèle dénombrable $\mathfrak{M}_2$ de $T \cup \{\neg F\}$. La formule F ne fait intervenir qu'un nombre fini de symboles, donc il existe un entier n tel que $F \in L_n$. On vient de voir que $\mathfrak{M}_1 \upharpoonright L_n$ et $\mathfrak{M}_2 \upharpoonright L_n$ sont isomorphes, ce qui est contradictoire avec le fait que l'un satisfait F et l'autre $\neg F$.

5. a) Soient λ un cardinal infini et $\mathfrak{M} = \langle M, \ldots \rangle$ une λ-structure ; M est donc un ensemble infini. La valeur dans $\mathfrak{M}$ de la formule $x \simeq x$ est M. Ce n'est pas un ensemble fini ; c'est donc un ensemble de cardinal λ.

b) Dans une structure $\mathfrak{M} = \langle M, \ldots \rangle$ de cardinal $\aleph_0$, toute partie de M est : soit finie, soit de cardinal $\aleph_0$. C'est en particulier vrai pour les parties de M qui sont valeur dans $\mathfrak{M}$ d'une formule de $\mathscr{F}_1$; $\mathfrak{M}$ est donc une $\aleph_0$-structure.

c) Soit λ un cardinal infini. Ajoutons à L un ensemble C de nouveaux symboles de constante, de cardinal λ, et considérons, dans le langage enrichi, la théorie :

$$T_F = T \cup \{F[c] \,;\, c \in C\} \cup \{\neg c \simeq d \,;\, c \neq d,\ c, d \in C\}.$$

Il est clair que le réduit au langage L de tout modèle de T' est un modèle de T dans lequel la valeur de la formule F a un cardinal supérieur ou égal à λ. Un argument élémentaire de compacité montre que T_F a au moins un modèle : il suffit de montrer que pour tout sous-ensemble fini C_0 de C, la théorie

$$T' = T \cup \{F[c] \,;\, c \in C_0\} \cup \{\neg c \simeq d \,;\, c \neq d,\ c, d \in C_0\}$$

a un modèle. Par hypothèse, il existe un modèle $\mathfrak{M}$ de T tel que $Val(F,\mathfrak{M})$ à une cardinalité supérieure à celle de C_0. On enrichit $\mathfrak{M}$ en un modèle de T' en interprétant les symboles appartenant à C_0 par des points distincts de $Val(F,\mathfrak{M})$ (il y en a assez), les autres constantes de C étant interprétées arbitrairement.

D'après le théorème de Lowenheim-Skolem descendant, on peut trouver un modèle $\mathfrak{N}$ de T_F dont le cardinal est celui du langage enrichi, c'est-à-dire λ (L étant dénombrable). La valeur de F dans $\mathfrak{N}$ ne peut être que de cardinal λ. Le réduit de $\mathfrak{N}$ au langage L est donc un modèle de T qui répond à la question.

d) Soient λ un cardinal infini et $\mathfrak{M}_0$ un modèle infini de T. Posons :

$$A = \{G \in \mathscr{F}_1 \,;\, Val(G,\mathfrak{M}_0) \text{ est infini}\} \,;$$

pour chaque formule F de A, soit un ensemble C_F de symboles de constante de cardinalité λ, ces ensembles étant choisis de telle sorte que si F et G sont deux éléments distincts de A, alors C_F et C_G sont disjoints. Pour $F \in A$, on considère la théorie suivante :

$$T_F = T \cup \{F[c]\ ;\ c \in C_F\} \cup \{\neg c \simeq d\ ;\ c \neq d,\ c, d \in C_F\}$$

et $$T' = Th(\mathfrak{M}) \cup \bigcup_{F \in A} T_F.$$

On va d'abord montrer que T' est consistante : par compacité, il suffit de montrer que si A_0 est un sous-ensemble fini de A et si, pour tout $F \in A_0$, D_F est un sous-ensemble fini de de C_F, alors

$$T'' = Th(\mathfrak{M}) \cup \{F(c)\ ;\ F \in A_0 \text{ et } c \in D_F\} \cup \{\neg c \simeq d\ ;\ \text{il existe } F \in A_0 \text{ tel que } c, d \in D_F\}$$

a un modèle. On peut enrichir $\mathfrak{M}$ en un modèle de T" : il suffit d'interpréter, pour chaque $F \in A_0$ les symboles de D_F (qui sont en nombre fini) par des points distincts de $Val(F,\mathfrak{M})$ (qui est un ensemble infini).

On voit donc que T' a un modèle, et comme à la question c), il a un modèle de cardinalité λ. Soient $\mathfrak{N}'$ un tel modèle et $\mathfrak{N}$ son réduit à L. On va montrer que $\mathfrak{N}$ est un λ-modèle : soit $F \in \mathcal{F}_1$; si $F \in A$, alors, par construction la cardinalité de $Val(F,\mathfrak{N})$ est égale à λ. Si $F \notin A$, alors $Val(F,\mathfrak{M})$ a un nombre fini, disons n, d'éléments. Donc la formule close

$$H = \forall v_0 \forall v_1 \ldots \forall v_n \Big(\bigwedge_{0 \leq i \leq n} F(v_i) \Rightarrow \bigvee_{0 \leq i < j \leq n} v_i = v_j\Big)$$

est vraie dans $\mathfrak{M}$, donc aussi dans $\mathfrak{N}$ qui a la même théorie : $Val(F,\mathfrak{N})$ est fini et $\mathfrak{N}$ est un λ modèle.

e) On raisonne par l'absurde : supposons que S ne soit pas complète ; il y a alors une formule close F de L telle que les théories $S \cup \{F\}$ et $S \cup \{\neg F\}$ soient toutes deux non contradictoires ; elles n'ont, comme S, que des modèles infinis ; d'après la question d), chacune de ces deux théories admet donc un λ-modèle, quel que soit le cardinal infini λ ; si on choisit λ de telle sorte que tous les λ-modèles de S soient isomorphes, on aboutit à une contradiction puisque, parmi tous ces λ-modèles isomorphes, il faudrait qu'il y en ait au moins un qui satisfasse F et au moins un qui satisfasse $\neg F$, ce qui est impossible. La théorie S est donc complète.

6. a) La structure $\langle \mathbb{Z}, n \mapsto n+1 \rangle$ est visiblement un modèle de T_1, que nous appellerons le modèle standard. Dans tout modèle $\mathfrak{M} = \langle M, \varphi \rangle$ de T_1, on peut définir une relation d'équivalence $\sim$ par : $a \sim b$ si et seulement si il existe un entier $n \in \mathbb{N}$ tel que $a = \varphi^n(b)$ ou $b = \varphi^n(a)$. Appelons orbite de a la classe de a pour la relation $\sim$. Chaque orbite définit une sous-structure de $\mathfrak{M}$ qui est un modèle de T_1 isomorphe au modèle standard. Pour que deux modèles de T_1 soient isomorphes, il faut et il suffit que leurs ensembles d'orbites soient équipotents. Si κ est un cardinal infini non dénombrable, tout modèle de T_1 de cardinal κ a nécessairement un ensemble d'orbites de cardinal κ, puisque chaque orbite est dénombrable. On en déduit que la théorie T_1 est κ-catégorique et, puisque tous ses modèles sont infinis, qu'elle est complète (théorème de Vaught).

b) Un modèle $\mathfrak{M} = \langle M, \varphi, \Omega \rangle$ de T_2 est un modèle de T_1 agrémenté d'un « coloriage » (en deux couleurs) pour les orbites : en effet, chaque orbite est : soit incluse dans Ω (disons alors qu'elle est rouge), soit incluse dans $M - \Omega$ (disons alors qu'elle est jaune) ; la formule $\forall x (Px \Longleftrightarrow Pfx)$ exclut toute autre possibilité ; de plus, les deux couleurs sont effectivement représentées ($\exists x Px$, $\exists x \neg Px$). Pour que deux modèles de T_2 soient isomorphes, il faut et il suffit que leurs ensembles d'orbites rouges soient équipotents, ainsi que leurs ensembles d'orbites jaunes. Soit κ un cardinal infini quelconque ; on obtient deux modèles de T_2 de cardinal κ non isomorphes en considérant, d'une part un modèle à une orbite rouge et κ orbites jaunes, et, d'autre part, un modèle à une orbite jaune et κ orbites rouges (de façon précise, on peut prendre $M = \mathbb{Z} \times \kappa$; $\varphi = (n, \alpha) \longmapsto (n+1, \alpha)$; $\Omega_1 = \mathbb{Z} \times \{0\}$ et $\Omega_2 = \mathbb{Z} \times (\kappa - \{0\})$; puis :

$$\mathfrak{M}_1 = \langle M, \varphi, \Omega_1 \rangle \text{ et } \mathfrak{M}_2 = \langle M, \varphi, \Omega_2 \rangle).$$

On voit que T_2 n'est pas κ-catégorique.

c) Soient λ un cardinal non dénombrable et $\mathfrak{M} = \langle M, \varphi, \Omega \rangle$ un λ-modèle de T_2 (voir l'exercice précédent, en particulier la question d)). La valeur de la formule Px dans $\mathfrak{M}$ n'est pas un ensemble fini (il y a au moins une orbite incluse dans Ω, c'est-à-dire une orbite rouge) ; on en déduit (parce que $\mathfrak{M}$ est un λ-modèle) que $\mathrm{Val}(Px, \mathfrak{M})$ est un ensemble de cardinal λ. Un raisonnement analogue vaut pour la formule $\neg Px$. Il en résulte que l'ensemble des orbites rouges et l'ensemble des orbites jaunes de $\mathfrak{M}$ sont de cardinal λ (parce que chaque orbite est dénombrable alors que λ ne l'est pas). On en déduit, comme dans la question b), que tous les λ-modèles de T_2 sont isomorphes, ce qui prouve, grâce à la dernière question de l'exercice 6, que T_2 est complète (il est clair que T_2 n'a pas de modèles finis).

7. a) Les modèles de T_0 sont les ensembles totalement ordonnés dans lesquels tout élément admet un successeur (c'est-à-dire un plus petit majorant strict) et un prédécesseur (c'est-à-dire un plus grand minorant strict).

Posons $\mathfrak{M}_0 = \langle 2\mathbb{Z}, \leqslant \rangle$ et $\mathfrak{M}_1 = \langle \mathbb{Z}, \leqslant \rangle$ ($2\mathbb{Z}$ est l'ensemble des entiers relatifs pairs) ; $\mathfrak{M}_0$ et $\mathfrak{M}_1$ sont clairement des modèles de T_0 (dans $\mathfrak{M}_0$, le successeur et le prédécesseur de l'élément $2k$ sont respectivement $2k+2$ et $2k-2$; dans $\mathfrak{M}_1$, le successeur et le prédécesseur de l'élément h sont respectivement $h+1$ et $h-1$) ; $\mathfrak{M}_0$ est une sous-structure de $\mathfrak{M}_1$, mais n'en est pas une sous-structure élémentaire, car, par exemple, la formule à paramètres dans $\mathfrak{M}_0$: $\forall v_0 (Rv_0 0 \vee R2v_0)$, est satisfaite dans $\mathfrak{M}_0$ mais pas dans $\mathfrak{M}_1$ ($\mathfrak{M}_1$ ne satisfait ni $R10$ ni $R21$).

b) Pour chaque entier $i \in \mathbb{N}$, posons :

$$M_i = \{x \in \mathbb{Q} \ ; \ 2^i x \in \mathbb{Z}\}, \text{ et } \mathfrak{M}_i = \langle M_i, \leqslant \rangle.$$

(L'ordre considéré est l'ordre usuel de $\mathbb{Q}$; M_i est l'ensemble des rationnels de la forme $a/2^i$, où $a \in \mathbb{Z}$; $\mathfrak{M}_i$ est une L_0-structure). Il est clair que, pour $i \leqslant j$, $\mathfrak{M}_i$ est une sous-structure de $\mathfrak{M}_j$. D'autre part, chaque $\mathfrak{M}_i$ est un modèle de T_0, en fait isomorphe à

$\mathfrak{M}_0$ (l'application qui, à tout $a \in \mathbb{Z}$ fait correspondre $a/2^i$ est un isomorphisme de $\mathfrak{M}_0$ sur $\mathfrak{M}_i$). On est donc en présence d'une chaîne de modèles de T_0. La réunion de cette chaîne est l'ensemble M des rationnels dont le dénominateur est une puissance de deux, muni de l'ordre usuel ; ce n'est pas un modèle de T_0 car, quels que soient les éléments a et b de M tels que $a < b$, b ne saurait être le successeur de a, car le rationnel $\frac{a+b}{2}$, qui appartient à M, est strictement compris entre a et b.

Grâce au théorème 5.6, nous pouvons donc conclure que T_0 n'est équivalente à aucune théorie $\forall\exists$ de L_0.

8. a) Soit $\mathfrak{M}$ un modèle premier d'une théorie modèle-complète T. Etant donnés deux modèles quelconques $\mathfrak{A}$ et $\mathfrak{B}$ de T, il existe des structures $\mathfrak{A}'$ et $\mathfrak{B}'$, respectivement isomorphes à $\mathfrak{A}$ et $\mathfrak{B}$ (donc modèles de T), telles que $\mathfrak{M} \subseteq \mathfrak{A}'$ et $\mathfrak{M} \subseteq \mathfrak{B}'$. Comme T est modèle-complète, on en déduit que ces inclusions sont élémentaires : $\mathfrak{M} \prec \mathfrak{A}'$ et $\mathfrak{M} \prec \mathfrak{B}'$. En particulier, $\mathfrak{A}'$ et $\mathfrak{B}'$ sont élémentairement équivalentes à $\mathfrak{M}$, donc $\mathfrak{A}' \equiv \mathfrak{B}'$. Or $\mathfrak{A}$ est isomorphe à $\mathfrak{A}'$ et $\mathfrak{B}$ à $\mathfrak{B}'$; on en conclut que $\mathfrak{A} \equiv \mathfrak{B}$. Ainsi, deux modèles quelconques de T sont élémentairement équivalents : T est complète.

b) 1°) implique 2°). On va plutôt montrer que la négation de 2°) implique la négation de 1°) : soient $\mathfrak{M}$ un modèle de T et F une formule close de L_M (le langage L auquel on a ajouté un symbole de constante pour chaque point de M) tels que F ne soit pas conséquence de $T \cup \Delta(\mathfrak{M})$; il existe donc un modèle $\mathfrak{M}'$ de $T \cup \Delta(\mathfrak{M}) \cup \{\neg F\}$, et on peut même supposer que $\mathfrak{M} \subseteq \mathfrak{M}'$ (voir 2.3). Pourtant, $\mathfrak{M}'$ n'est pas une extension élémentaire de $\mathfrak{M}$ puisque F est satisfaite dans $\mathfrak{M}$ mais pas dans $\mathfrak{M}'$.

2°) implique 1°). Supposons que $\mathfrak{M} \subseteq \mathfrak{M}'$ soient deux modèles de T. Alors $\mathfrak{M}'$, lorsqu'on l'a enrichi en une L_M-structure de façon naturelle, est un modèle de $T \cup \Delta(\mathfrak{M})$, donc un modèle de $D(\mathfrak{M})$. Il en découle que $\mathfrak{M} \prec \mathfrak{M}'$.

2°) implique 3°) est évident.

3°) implique 2°). On démontre encore que la négation de 2°) implique la négation de 3°) : Soient $\mathfrak{M}$ un modèle de T et F une formule de $D(\mathfrak{M})$ qui n'est pas conséquence de $T \cup \Delta(\mathfrak{M})$. Il existe donc une formule $G[v_0,v_1,\dots,v_n]$ de L et des éléments $a_1, a_2, \dots, a_n$ de M tel que $F = G[a_0,a_1,\dots,a_n]$ et $\mathfrak{M} \models F$. Par le théorème 1.5, il existe une extension élémentaire dénombrable $\mathfrak{M}_0$ de $\mathfrak{M}$ ccontenant les éléments $a_1, a_2, \dots, a_n$. Comme F n'est pas conséquence de $T \cup \Delta(\mathfrak{M})$, ce n'est pas non plus une conséquence de $T \cup \Delta(\mathfrak{M}_0)$, qui en est un sous-ensemble. Il existe donc un modèle $\mathfrak{M}_1$ dénombrable de $T \cup \Delta(\mathfrak{M}_0) \cup \{\neg F\}$, et on peut même supposer que $\mathfrak{M}_0 \subseteq \mathfrak{M}_1$; $\mathfrak{M}_0$ satisfait F, parce que c'est une sous-structure élémentaire de $\mathfrak{M}$ et $\mathfrak{M}_1$ ne satisfait pas F : T n'est pas modèle complète.

1°) implique 4°) est évident.

4°) implique 3°) se démontre comme 1°) implique 2°), en ne choisissant que des modèles dénombrables, ce que le théorème de Lowenheim-Skolem permet de faire.

c) On utilise le théorème 5.6 : il suffit de montrer que la classe des modèles de T est close par union de chaîne. Or d'après la modèle complétude, toute chaîne de modèles est une chaîne élémentaire. L'union d'une chaîne de modèles de T est donc un modèle de T d'après le théorème 2.9.

d) La condition (*) est vérifiée pour les formules existentielles (voir le corollaire 5.3), et aussi pour les formules équivalentes modulo T à une formule existentielle. Cela démontre le sens « si ».

Pour l'autre sens, on ajoute, comme il est suggéré, des nouveaux symboles de constante $c_0, c_1, \ldots, c_n$ au langage, et on considère la théorie :

$$\Psi = \{ G[c_0,c_1,\ldots,c_n] \text{ ; } G[v_0,v_1,\ldots,v_n] \text{ est une formule universelle de L et } T \vdash \neg F[c_0,c_1,\ldots,c_n] \Rightarrow G[c_0,c_1,\ldots,c_n] \}.$$

Soit $\mathfrak{N}$ un modèle de $T \cup \Psi$. On va voir que $\mathfrak{N}$ admet une extension $\mathfrak{N}'$ satisfaisant $\neg F[c_0,c_1,\ldots,c_n]$. On utilise pour cela la méthode des diagrammes : il suffit de montrer que $T \cup \Delta(\mathfrak{N}) \cup \neg F[c_0,c_1,\ldots,c_n]$ est consistante. On raisonne par l'absurde et on suppose le contraire : il existe une formule H de $\Delta(\mathfrak{N})$ telle que :

$$T \vdash H \Longrightarrow F[c_0,c_1,\ldots,c_n].$$

Comme H appartient à $\Delta(\mathfrak{N})$, il existe une formule $K[v_0,v_1,\ldots,v_{n+p}]$ de L sans quantificateur et des points $a_1, a_2, \ldots, a_p$ de N tels que $H = K[c_0,c_1,\ldots,c_n,a_1,a_2,\ldots,a_p]$. Comme les points a_i, pour i compris entre 1 et p n'apparaissent ni dans T ni dans $F[c_0,c_1,\ldots,c_n]$, on en déduit que :

$$T \vdash \forall v_0 \forall v_1 \ldots \forall v_p (K[c_0,c_1,\ldots,c_n,v_1,v_2,\ldots,v_p] \Longrightarrow F[c_0,c_1,\ldots,c_n])$$

ou, ce qui est équivalent :

$$T \vdash \neg F[c_0,c_1,\ldots,c_n] \Longrightarrow \forall v_0 \forall v_1 \ldots \forall v_p \neg K[c_0,c_1,\ldots,c_n,v_1,v_2,\ldots,v_p]$$

On voit donc que la formule $\forall v_0 \forall v_1 \ldots \forall v_p \neg K[c_0,c_1,\ldots,c_n,v_1,v_2,\ldots,v_p]$ appartient à Ψ, donc est vraie dans $\mathfrak{N}$, ce qui est contradictoire avec le fait que $K[c_0,c_1,\ldots,c_n,a_1,a_2,\ldots,a_p]$ appartienne à $\Delta(\mathfrak{N})$.

Supposons maintenant que la formule $F[v_0,v_1,\ldots,v_n]$ satisfasse la condition (*). Comme un modèle de $T \cup F[c_0,c_1,\ldots,c_n]$ ne peut pas avoir d'extension satisfaisant $\neg F[c_0,c_1,\ldots,c_n]$, il découle de ce qui précède que $T \cup F[c_0,c_1,\ldots,c_n] \cup \Psi$ est contradictoire. Par compacité, il existe donc une partie finie Ψ_0 de Ψ telle que $\neg F[c_0,c_1,\ldots,c_n]$ soit conséquence de $\Psi_0 \cup T$, et, puisque Ψ_0 est conséquence de $T \cup \neg F[c_0,c_1,\ldots,c_n]$ on a :

$$T \vdash \neg F[c_0,c_1,\ldots,c_n] \Longleftrightarrow \bigwedge_{G \in \Psi_0} G[c_0,c_1,\ldots,c_n].$$

Or, on sait que la conjonction de formules universelles est équivalente à une formule universelle, et que la négation d'une formule universelle est équivalente à une formule existentielle. Il existe donc une formule existentielle $H[v_0,v_1,\ldots,v_n]$ de L telle que :

$$T \vdash F[c_0,c_1,\ldots,c_n] \Longleftrightarrow H[c_0,c_1,\ldots,c_n],$$

et, puisque les constantes c_i n'apparaissent pas dans T,

$$T \vdash \forall v_0 \forall v_1 \ldots \forall v_n (F[v_0,v_1,\ldots,v_n] \Longleftrightarrow H[v_0,v_1,\ldots,v_n]).$$

e) Dire que T est modèle-complète, c'est dire que la condition (*) est vérifiée pour toute formule de L. D'après d), il suffit donc de montrer : la condition (*) est vérifiée pour toutes les formules si et seulement si elle est vérifiée pour toutes les formules universelles.

Supposons que (*) est vérifiée pour les formules universelles ; on va montrer qu'elle est vérifiée pour toutes les formules. On raisonne par induction. Soit $F[v_0,v_1,\dots,v_n]$ une formule de L, et on peut supposer qu'il n'y a pas d'autres symboles logiques que $\neg$, $\wedge$, $\vee$, $\forall$ apparaissant dans $F[v_0,v_1,\dots,v_n]$. Seul le cas où $F[v_0,v_1,\dots,v_n] = \neg G[v_0,v_1,\dots,v_n]$ pose problème. Par hypothèse d'induction, on sait qu'il existe une formule existentielle $H[v_0,v_1,\dots,v_n]$ telle que

$$T \vdash \forall v_0 \forall v_1 \dots \forall v_n (H[v_0,v_1,\dots,v_n] \Longleftrightarrow G[v_0,v_1,\dots,v_n]),$$

donc $T \vdash \forall v_0 \forall v_1 \dots \forall v_n (\neg H[v_0,v_1,\dots,v_n] \Longleftrightarrow \neg G[v_0,v_1,\dots,v_n])$.

Or, $\neg H[v_0,v_1,\dots,v_n]$ est équivalente à une formule universelle, et, par hypothèse, il existe une formule existentielle $K[v_0,v_1,\dots,v_n]$ telle que :

$$T \vdash \forall v_0 \forall v_1 \dots \forall v_n (\neg H[v_0,v_1,\dots,v_n] \Longleftrightarrow K[v_0,v_1,\dots,v_n]),$$

et il découle de tout ceci que :

$$T \vdash \forall v_0 \forall v_1 \dots \forall v_n (F[v_0,v_1,\dots,v_n] \Longleftrightarrow K[v_0,v_1,\dots,v_n]).$$

9. a) Le sens 2°) implique 1°) a été démontré au d) de l'exercice 8 ; dans l'autre sens, on reprend la preuve qui a été faite au d), en prenant soin de choisir tous les modèles dont on a besoin de cardinalité λ, ce qui est possible grâce au théorème de Lowenheim-Skolem.

b) On part d'un modèle $\mathfrak{M}$ de T de cardinalité λ. On va d'abord construire une extension $\mathfrak{M}^1$ de $\mathfrak{M}$ qui est un modèle de T et qui satisfait la condition suivante :

(1) pour tous éléments $a_0, a_1, \dots, a_n$ de M, pour tout modèle $\mathfrak{M}'$ de T qui est une extension de $\mathfrak{M}^1$,

$$\text{si } \mathfrak{M}^1 \models F[a_0,a_1,\dots,a_n] \text{ alors } \mathfrak{M}' \models F[a_0,a_1,\dots,a_n].$$

Pour cela, on énumère l'ensemble des suites de longueur n d'éléments de M (cet ensemble est de cardinalité λ) : $\{(a_0^i,a_1^i,\dots,a_n^i) ; i \in \lambda\}$. Le modèle $\mathfrak{M}^1$ sera la réunion d'une chaîne croissante de modèles de T, $(\mathfrak{M}_i ; i \in \lambda)$, que l'on va construire par induction sur $i \in \lambda$, de la façon suivante :

– $\mathfrak{M}_0 = \mathfrak{M}$;

– si i est un ordinal limite, $\mathfrak{M}_i = \bigcup_{j<i} \mathfrak{M}_j$; on sait que $\mathfrak{M}_i$ est un modèle de T parce que T est $\forall\exists$ (théorème 5.6);

– supposons que $i = j + 1$; on distinguera plusieurs cas :

α) si $\mathfrak{M}_j \models \neg F[a_0^j,a_1^j,\dots,a_n^j]$, alors on pose $\mathfrak{M}_i = \mathfrak{M}_j$; on remarque que puisque F est universelle, pour toute extension $\mathfrak{N}$ de $\mathfrak{M}_i$ (et en particulier pour le modèle $\mathfrak{M}^1$ que l'on obtiendra à la fin de cette construction), $\mathfrak{N} \models \neg F[a_0^j,a_1^j,\dots,a_n^j]$.

β) si $\mathfrak{M}_j \models F[a_0^j,a_1^j,\dots,a_n^j]$, et si pour tout $\mathfrak{N}$ modèle de T qui est une extension de $\mathfrak{M}_j$, $\mathfrak{N} \models F[a_0^j,a_1^j,\dots,a_n^j]$, alors on pose encore $\mathfrak{M}_i = \mathfrak{M}_j$; ici encore, on

remarque que cette propriété sera vrai pour $\mathfrak{M}^1$: pour tout $\mathfrak{N}$ modèle de T qui est une extension de $\mathfrak{M}^1$, $\mathfrak{N} \models F[a_0^j,a_1^j,\ldots,a_n^j]$;

γ) reste le cas où $\mathfrak{M}_j \models F[a_0^j,a_1^j,\ldots,a_n^j]$, et qu'il existe un modèle $\mathfrak{N}$ de T qui est une extension de $\mathfrak{M}_j$ telle que $\mathfrak{N} \models \neg F[a_0^j,a_1^j,\ldots,a_n^j]$; dans ce cas, $\mathfrak{M}_i$ sera un tel modèle de dont la cardinalité est λ (qui existe par le théorème de Lowenheim-Skolem).

En posant, comme annoncé, $\mathfrak{M}^1 = \bigcup_{j<\lambda} \mathfrak{M}_j$, on obtient un modèle de T de cardinalité λ et satisfaisant la propriété (1).

On recommence : on construit par la même méthode un modèle $\mathfrak{M}^2$ tel que :

pour tous éléments $a_0, a_1, \ldots, a_n$ de M_1, pour tout modèle $\mathfrak{M}'$ de T qui est une extension de $\mathfrak{M}^2$,

si $\mathfrak{M}^2 \models F[a_0,a_1,\ldots,a_n]$ alors $\mathfrak{M}' \models F[a_0,a_1,\ldots,a_n]$,

puis un modèle $\mathfrak{M}^3$ etc. Si on pose $\mathfrak{M}' = \bigcup_{k\in\mathbb{N}} \mathfrak{M}^k$, on voit que $\mathfrak{M}'$ est un modèle de T (toujours parce que T est $\forall\exists$), de cardinalité λ, et qu'il satisfait la condition ($\bullet$) requise par l'énoncé (parce qu'une suite finie d'éléments de M' se trouve déjà dans un ensemble M^k, pour un entier k).

c) On vient de voir que si T est $\forall\exists$, alors il en existe un modèle $\mathfrak{M}$ de cardinalité λ satisfaisant ($\bullet$) ; si de plus T est λ-catégorique, alors tous les modèles de cardinalité λ sont isomorphes à $\mathfrak{M}$, et satisfont aussi ($\bullet$) : donc la condition 1°) de a) est vérifiée pour toute formule universelle $F[v_0,v_1,\ldots,v_n]$. Il découle alors du d) de l'exercice 8 que toute formule universelle est équivalente modulo T à une formule existentielle, et donc, avec le e) du même exercice, T est modèle-complète.

d) La théorie T_0 n'est pas modèle-complète : soient $\mathfrak{M}_0$ le modèle dont l'ensemble de base est l'ensemble $\mathbb{N}$ et où l'interprétation de f est l'application $\lambda n.n+1$ et $\mathfrak{M}_1$ le modèle dont l'ensemble de base est l'ensemble $\mathbb{Z}$ et où l'interprétation de f est encore l'application $\lambda n.n+1$. Alors $\mathfrak{M}_0$ est une sous-structure de $\mathfrak{M}_1$, mais n'en est pas une sous-structure élémentaire ($\exists v_0(0 \simeq fv_0)$ est vraie dans $\mathfrak{M}_1$ mais pas dans $\mathfrak{M}_0$).

REMARQUE : Cet exemple est destiné à montrer que la condition « T est $\forall\exists$ » n'implique pas « T est modèle complète ». La question qu'il est naturel de se poser, surtout après le théorème de Lindström et la question c) de l'exercice 8, est : une théorie complète $\forall\exists$ est-elle nécessairement modèle-complète ? (T_0 n'est pas complète : l'interprétation de f peut être bijective ou ne pas l'être). Le lecteur que cette question angoisse méditera l'exemple suivant : on ajoute au langage de T_0 une infinité dénombrable de symboles de constante $c_0, c_1, \ldots$ et on considère la théorie T constitué de T_0 et de l'ensemble :

$$\{\forall v_0 \neg c_n \simeq fv_0 \,;\, n \in \mathbb{N}\} \cup \{c_n \neq c_m \,;\, n \neq m,\ n, m \in \mathbb{N}\}.$$

La théorie T est complète, $\forall\exists$ (en fait, elle est même universelle), mais elle n'est pas modèle-complète. Le plus difficile est de montrer qu'elle est complète. Pour cela, on procède à une analyse des modèles de T (c'est la méthode qui nous a réussi pour un

grand nombre de ces exercices) : un modèle $\mathfrak{M} = < M, \mathfrak{f}, \bar{c}_n >$ se décompose en $\mathfrak{f}$-orbites (une $\mathfrak{f}$-orbite est une classe d'équivalence pour la relation : il existe des entiers n et m tels que $\mathfrak{f}^n(x) = \mathfrak{f}^m(y)$), et il y a trois sortes d'orbites : celles des éléments $\bar{c}_n$; celles sur lesquelles la restriction de $\mathfrak{f}$ est bijective ; les autres. Le lecteur pourra démontrer d'une part que deux modèles dénombrables qui possèdent une infinité dénombrable d'orbites de chaque sorte sont isomorphes et d'autre part, que tout modèle dénombrable admet une extension élémentaire ayant un nombre dénombrable d'orbites de chaque sorte.

10. Appelons L_0 le langage réduit au seul symbole R. Nous utiliserons les faits suivants : tout modèle dénombrable de A est isomorphe à l'ensemble ordonné des rationnels (voir 2.7) ; si $\mathfrak{M}$ et $\mathfrak{N}$ sont deux modèles de A et si $(m_0, m_1, \ldots, m_k)$ et $(n_0, n_1, \ldots, n_k)$ sont deux suites d'éléments de M et N respectivement, alors les deux conditions suivantes sont équivalentes :

1°) Pour toute formule $F[v_0, v_1, \ldots, v_k]$ de L_0,

$$\mathfrak{M} \models F[m_0, m_1, \ldots, m_k] \text{ si et seulement si } \mathfrak{N} \models F[n_0, n_1, \ldots, n_k] ;$$

2°) Pour toute formule sans quantificateur $F[v_0, v_1, \ldots, v_k]$ de L_0,

$$\mathfrak{M} \models F[m_0, m_1, \ldots, m_k] \text{ si et seulement si } \mathfrak{N} \models F[n_0, n_1, \ldots, n_k].$$

(lemme 2 de 1.3)

Par ailleurs, voici quelques remarques à propos des suites α, β et γ : ce sont trois suites strictement croissantes de rationnels ; la première n'est pas majorée, la deuxième est majorée et admet une borne supérieure qui est le rationnel 1, la troisième est majorée mais n'admet pas de borne supérieure dans $\mathbb{Q}$ (sa borne supérieure dans $\mathbb{R}$ étant le nombre e qui n'est pas rationnel).

a) Soient $\mathfrak{M}$ et $\mathfrak{N}$ deux modèles de T et appelons, pour chaque $k \in \mathbb{N}$, m_k et n_k les interprétations de c_k dans $\mathfrak{M}$ et $\mathfrak{N}$ respectivement. Soit F une formule close de L. Il existe alors un entier k et une formule $G[v_0, v_1, \ldots, v_k]$ de L_0 telle que $F = G[c_0, c_1, \ldots, c_k]$. Puisque les suites $(m_0, m_1, \ldots, m_k)$ et $(n_0, n_1, \ldots, n_k)$ sont toutes les deux strictement croissantes, elles vérifient la conditions 2°) ci-dessus, et donc aussi la condition 1°) ; autrement dit :

$$\mathfrak{A} \models G[c_0, c_1, \ldots, c_k] \text{ si et seulement si } \mathfrak{B} \models G[c_0, c_1, \ldots, c_k].$$

Les structures $\mathfrak{M}$ et $\mathfrak{N}$ vérifient les mêmes formules closes et sont donc élémentairement équivalentes : la théorie T est complète.

b) Soit $\mathfrak{M}$ un modèle dénombrable de T. Alors $\mathfrak{M}{\restriction}L_0$ est un modèle dénombrable de A, et il existe donc un isomorphisme φ de $\mathfrak{M}{\restriction}L_0$ sur $(\mathbb{Q}, \leqslant)$. On peut enrichir $(\mathbb{Q}, \leqslant)$ en une L-stucture $\mathfrak{M}_1$ en décrétant que, pour tout $n \in \mathbb{N}$, l'interprétation de c_n est l'image par φ de l'interprétation de c_n dans $\mathfrak{M}$. Ainsi, on est assuré que φ est un isomorphisme de $\mathfrak{M}$ sur $\mathfrak{M}_1$.

Il ne reste plus qu'à montrer que $\mathfrak{M}_1$ est isomorphe à l'une des trois structures $\mathfrak{A}$, $\mathfrak{B}$, ou $\mathfrak{C}$. Appelons δ_n l'interprétation de c_n dans $\mathfrak{M}_1$. Alors $\Delta = (\delta_n \; ; \; n \in \mathbb{N})$ est une suite

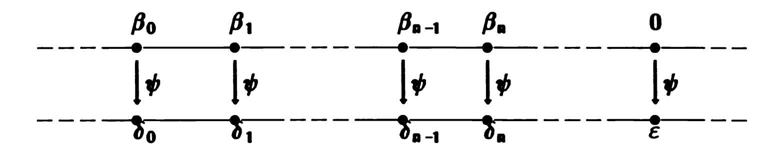
de rationnels strictement croissante et trois cas peuvent se présenter :

1°) La suite Δ n'est pas majorée. Voici un isomorphisme ψ de $\mathfrak{A}$ sur $\mathfrak{M}_1$: soit $x \in \mathbb{Q}$;

– si $x \leqslant 0$, alors $\psi(x) = x + \delta_0$ (ainsi ψ est une application croissante et bijective de l'intervalle $]-\infty,\alpha_0]$ sur l'intervalle $]-\infty,\delta_0]$.)

- si $n \leqslant x \leqslant n+1$, alors $\psi(x) = \gamma_{n+1} - \gamma_n)(x-n) + \gamma_n$ (ψ est donc encore une application croissante de $[\alpha_n,\alpha_{n+1}]$ sur $[\delta_n,\delta_{n+1}]$.

2°) La suite Δ est majorée et sa borne supérieure est un nombre rationnel ε. Cette fois-ci, c'est $\mathfrak{B}$ qui est isomorphe à $\mathfrak{M}_1$; l'isomorphisme ψ de $\mathfrak{B}$ sur $\mathfrak{M}_1$ est construit suivant le même principe : on met en bijection les intervalles que découpent sur $\mathbb{Q}$ les suites $(\alpha_n\ ;\ n \in \mathbb{N})$ et $(\delta_n\ ;\ n \in \mathbb{N})$ respectivement :



– si $x \leqslant \beta_0$, alors $\psi(x) = x - \beta_0 + \delta_0$;
- si $\beta_n \leqslant x \leqslant \beta_{n+1}$, alors $\psi(x) = \dfrac{\delta_{n+1} - \delta_n}{\beta_{n+1} - \beta_n}(x - \beta_n)$;
-si $x \geqslant 0$, $\psi(x) = x + \varepsilon$.

3°) La suite Δ est majorée et sa borne supérieure est un nombre irrationnel ε. On définit l'application de $\mathfrak{C}$ dans $\mathfrak{M}_1$ par :

– si $x \leqslant \gamma_0$, alors $\psi(x) = x - \gamma_0 + \delta_0$;
- si $\beta_n \leqslant x \leqslant \beta_{n+1}$, alors $\psi(x) = \dfrac{\delta_{n+1} - \delta_n}{\gamma_{n+1} - \gamma_n}(x - \gamma_n)$;

- il reste à définir ψ sur $\mathbb{Q} \cap]e,+\infty]$: il existe un isomorphisme θ de cet intervalle sur $\mathbb{Q} \cap]\varepsilon,+\infty]$ (parce qu'il s'agit de deux ordres totaux, denses, dénombrables, sans premier ni dernier élément). On pose $\psi(x) = \theta(x)$.

Il est à peu près évident que les trois structures $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ sont deux à deux non isomorphes : la conclusion est que T admet, à isomorphisme près, trois modèles dénombrables $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$.

c) Découle à peu près immédiatement du lemme 2 de 1.3.

d) Puisque T est modèle-complète, nous pouvons remplacer dans la question posée « extension élémentaire » par « extension (simple) ». De plus, il suffit de montrer que $\mathfrak{A}$ admet une extension isomorphe à $\mathfrak{B}$, que $\mathfrak{B}$ admet une extension isomorphe à $\mathfrak{C}$ et que $\mathfrak{C}$ admet une extension isomorphe à $\mathfrak{B}$.

Au lieu de montrer que $\mathfrak{A}$ admet une extension isomorphe à $\mathfrak{B}$, on peut montrer que $\mathfrak{B}$ admet une sous-structure isomorphe à $\mathfrak{A}$ (grâce à un raisonnement analogue à celui du lemme 2.3) : si $\mathfrak{B}_0$ est la sous-structure de $\mathfrak{B}$ dont la base est l'intervalle

$]-\infty,0]$, on voit que $\mathfrak{B}_0$ est un modèle de T dans lequel la suite $(\beta_n\ ;\ n \in \mathbb{N})$ n'est pas majorée, donc isomorphe à $\mathfrak{A}$ d'après ce qui a été dit en b).

De même, il y a une sous-structure $\mathfrak{C}_0$ de $\mathfrak{C}$ isomorphe à $\mathfrak{B}$; c'est celle dont l'ensemble de base est $]-\infty,e[\cup [3,+\infty[$: $\mathfrak{C}_0$ est bien un modèle de T, et, dans $\mathfrak{C}_0$, la suite $(\gamma_n\ ;\ n \in \mathbb{N})$ est majorée et admet une borne supérieure, à savoir **3**.

On peut par ailleurs trouver une extension dénombrable de $\mathfrak{C}$ qui soit un modèle de T et dans laquelle la suite $(\gamma_n\ ;\ n \in \mathbb{N})$ admette une borne supérieure : c'est la sous-structure de $(\mathbb{R},\leqslant)$ dont l'ensemble de base est $\mathbb{Q} \cup \{e\}$.

11. a) Soit $\mathfrak{M} = \langle M, \bar{f}, \bar{R} \rangle$ un modèle de A. La première formule exprime que la relation $\leqslant$ est réflexive la deuxième qu'elle est antisymétrique et totale (si x et y sont deux éléments distincts de M, une et une seule des deux propriétés $\bar{R}xy$ et $\bar{R}yx$ est vraie) ; la troisième formule exprime la transitivité de $\bar{R}$; il s'agit donc d'un ordre total. Ceci, plus la quatrième formule implique que $\bar{f}$ est un isomorphisme de la structure $\langle M, \bar{R} \rangle$ sur elle-même. D'après les cinquième et sixième formules, pour tout élément x, $\bar{f}(x)$ majore strictement x et est son successeur, c'est-à-dire le plus petit de ses majorants stricts.

b) La vérification ne pose aucun problème.

c) Le fait que la relation $\ll$ est transitive et réflexive découle facilement des propriétés de f et de $\bar{R}$. Le fait que la relation $\approx$ soit une relation d'équivalence est à peu près évident

Si $a \approx b$, alors il existe des entiers n et p tels que $\bar{f}^n(a) = \bar{f}^p(b)$. On a alors :

$$\mathfrak{M} \models \neg R f^{n+1} a\, b \wedge \neg R f^{p+1} b\, a,$$

et il est faux que $a \ll b$ et que $b \ll a$. Réciproquement, si $a \ll b$ et $b \ll a$ sont tous deux faux, alors il existe des entiers n et p tels que :

$$\mathfrak{M} \models \neg R f^n a\, b \wedge \neg R f^p b\, a\ .$$

Supposons par exemple que a soit inférieur ou égal à b (pour $\bar{R}$), et soit m le plus petit entier tel que $\mathfrak{M} \models \neg R f^m a\, b$; m est stictement positif et $\mathfrak{M} \models R f^{m-1} a\, b$. Comme $\bar{f}^m(a)$ est le successeur de $\bar{f}^{m-1}(a)$, on voit que $\bar{f}^m(a) = b$ (sinon, on aurait aussi $\mathfrak{M} \models R f^m a\, b$) : on a bien : $a \approx b$.

Comme $\bar{f}$ est bijective, on peut parler de son application réciproque $\bar{f}^{-1}$, et même de l'application $\bar{f}^n$ pour tout $n \in \mathbb{Z}$.

Soit a un élément de M. On vérifie que l'application de $\mathbb{Z}$ dans M qui à $n \in \mathbb{Z}$ fait correspondre $\bar{f}^n(a)$ est un monomorphisme de $\mathbb{Z}$ dans $\mathfrak{M}$, et que son image est la classe de a relativement à $\approx$. Il est par ailleurs facile de voir que cette classe est close par $\bar{f}$, ce qui montre que c'est une sous-structure de $\mathfrak{M}$.

On voit que si a, b et c sont des éléments de M, et que $a \approx b$, alors $a \ll c$ si et seulement si $b \ll c$: supposons par exemple que $a = \bar{f}^n(b)$, avec $n \in \mathbb{N}$. Il est alors bien clair que « pour tout $p \in \mathbb{N}$, $\bar{R}\bar{f}^p(b)c$ » est équivalent à « pour tout $p \in \mathbb{N}$, $\bar{R}\bar{f}^{n+p}(b)c$ »,

qui est lui-même équivalent à « pour tout $p \in \mathbb{N}$, $R\bar{f}^p(a)c$ » : ainsi, on peut définir une relation binaire $\lhd$ sur $M/\approx$ par : pour tous a, b appartenant à M, $a/\approx \lhd b/\approx$ si et seulement si $a \ll b$. Le fait que la relation $\lhd$ soit transitive et antiréflexive découle immédiatement des propriétés correspondantes de la relation $\ll$. Pour montrer que $\lhd$ est relation d'ordre stricte totale, il suffit de voir que si α et β sont des éléments de $M/\approx$, alors $\alpha = \beta$ ou $\alpha \lhd \beta$ ou $\beta \lhd \alpha$; autrement dit, que si a et b sont des éléments de M, alors $a \approx b$ ou $a \ll b$ ou $b \ll a$: c'est ce qu'on a fait au début de cette question.

Soient donc C l'ensemble $M/\approx$ et $X = (C, \lhd)$. Pour chaque $\alpha \in C$, choisissons un point c_α dans la classe α. Alors l'application φ de $\mathfrak{M}_X$ dans $\mathfrak{M}$ définie par : pour tout $\alpha \in C$, pour tout $n \in \mathbb{Z}$, $\varphi((\alpha,n)) = \bar{f}^n(c_\alpha)$ est un isomorphisme, comme cela se vérifie sans problème.

d) On laisse le lecteur vérifier les faits suivants :

- si φ est un isomorphisme entre les ensembles totalement ordonnés X et Y, alors l'application ψ de $\mathfrak{M}_X$ sur $\mathfrak{M}_Y$ définie par : pour tout $a \in X$, pour tout $n \in \mathbb{Z}$, $\psi((a,n)) = (\varphi(a),n)$ est un isomorphisme ;
- si ψ est un isomorphisme de $\mathfrak{M}_X$ sur $\mathfrak{M}_Y$, alors l'ensemble

$$\{ (a,b) \text{ ; il existe des } n \text{ et } p \text{ dans } \mathbb{Z} \text{ tels que } \psi((a,n)) = (b,p) \}$$

est le graphe d'un isomorphisme de X sur Y.

Si λ est un cardinal infini, on peut donc trouver deux modèles de A de cardinalité λ qui ne sont pas isomorphes : par exemple $X = \lambda$ et $Y = \lambda \cup \{ \lambda \}$ sont des ensembles totalement ordonnés non isomorphes (le premier ne possède pas d'élémenent maximum, le second en a un) de cardinalité λ. Donc $\mathfrak{M}_X$ et $\mathfrak{M}_Y$ ne sont pas isomorphes et sont tous les deux de cardinalité λ : A n'est catégorique en aucun cardinal infini.

e)

1°) On utilise la méthode des diagrammes : dans le langage L_M, on considère $D(\mathfrak{M})$, le diagramme complet de $\mathfrak{M}$ (voir 2.3) ; on ajoute un symbole de constante c, et on considère la théorie :

$$T = D(\mathfrak{M}) \cup \{\neg Rcf^n\underline{a} \text{ ; } n \in \mathbb{N}\} \cup \{\neg R\underline{b}f^n c \text{ ; } n \in \mathbb{N}\}.$$

On montre, à l'aide du théorème de compacité que cette théorie est consistante : si T_0 est un sous-ensemble fini de T, il existe un entier k tel que T_0 soit inclus dans :

$$D(\mathfrak{M}) \cup \{\neg Rcf^n\underline{a} \text{ ; } 0 \leqslant n < k\} \cup \{\neg R\underline{b}f^n c \text{ ; } 0 \leqslant n < k\}$$

et pour avoir un modèle de T_0, il suffit d'enrichir $\mathfrak{M}$ en interprétant c par $\bar{f}^{k+1}(a)$.

On a vu que T admet un modèle $\mathfrak{M}_1$ dont le réduit à L est une extension élémentaire de $\mathfrak{M}$. Si $\bar{c}$ est l'interprétation de c dans $\mathfrak{M}$, on a bien : $a \ll \bar{c}$ et $\bar{c} \ll b$.

2°) On fait un raisonnement analogue. Il faut montrer que la théorie

$$T_1 = D(\mathfrak{M}) \cup \{\neg Rcf^n\underline{a} < c \text{ ; } n \in \mathbb{N}\} \cup \{\neg Raf^n b < \underline{a} \text{ ; } n \in \mathbb{N}\},$$

dans un langage enrichi de deux nouveaux symboles de constante b et c est consistante.

3°) On laisse cette vérification au lecteur.

4°) Si, pour un indice i compris entre 1 et n, $c \approx a_i$, alors il existe un élément p de $\mathbb{Z}$ tel que $c = f^p(a_i)$. En se servant de 3°), on voit alors que :

$$P((\mathfrak{M}, a_1, a_2, \ldots, a_n, c), (\mathfrak{N}, b_1, b_2, \ldots, b_n, f^p(b_i)).$$

Dans le cas contraire, on distinguera plusieurs cas :

• Pour tout i compris entre 0 et n, $c \ll a_i$; on utilise alors 2°) pour trouver une extension élémentaire $\mathfrak{N}'$ de $\mathfrak{N}$ et et un point d de $\mathfrak{N}'$ tel que : pour tout i compris entre 0 et n, $d \ll a_i$. On a alors (toujours d'après 3°)) :

$$P((\mathfrak{M}, a_1, a_2, \ldots, a_n, c), (\mathfrak{N}', b_1, b_2, \ldots, b_n, d)).$$

• Pour tout i compris entre 0 et n, $a_i \ll c$. Cette fois-ci, on choisit $\mathfrak{N}' \succ \mathfrak{N}$ et d dans $\mathfrak{N}'$ tel que pour tout i compris entre 0 et n, $b_i \ll d$. On a encore :

$$P((\mathfrak{M}, a_1, a_2, \ldots, a_n, c), (\mathfrak{N}', b_1, b_2, \ldots, b_n, d)).$$

• Enfin, dans le cas restant, appelons a_i le plus grand des éléments de l'ensemble $\{a_1, a_2, \ldots, a_n\}$ qui est inférieur à c et a_j le plus petit qui est supérieur à c. On a alors : $a_i \ll c$ et $c \ll a_j$, et puisque $P((\mathfrak{M}, a_1, a_2, \ldots, a_n), (\mathfrak{N}, b_1, b_2, \ldots, b_n))$, $b_i \ll b_j$. On utilise 1°) pour trouver $\mathfrak{N}' \succ \mathfrak{N}$ et d dans $\mathfrak{N}$ tel que $b_i \ll d$ et $d \ll b_j$. Encore une fois, on a :

$$P((\mathfrak{M}, a_1, a_2, \ldots, a_n, c), (\mathfrak{N}', b_1, b_2, \ldots, b_n, d)).$$

5°) On peut toujours supposer que le quantificateur universel n'apparaît pas dans la formule $G[v_1, v_2, \ldots, v_n]$. Dans la démonstration par induction de l'assertion, les connecteurs propositionnels n'offrent aucune difficulté et l'hypothèse donne les formules atomiques. Ne reste que le quantificateur existentiel.

On suppose donc que $P((\mathfrak{M}, a_1, a_2, \ldots, a_n), (\mathfrak{N}, b_1, b_2, \ldots, b_n))$ est vérifiée, que $G[v_1, v_2, \ldots, v_n] = \exists v_0 F[v_0, v_1, \ldots, v_n]$ et que $\mathfrak{M} \models G[a_1, a_2, \ldots, a_n]$. Il existe donc un point c dans $\mathfrak{M}$ tel que $\mathfrak{M} \models F[c, a_1, a_2, \ldots, a_n]$. D'après la question 4°), il existe $\mathfrak{N}' \succ \mathfrak{N}$ et d dans $\mathfrak{N}'$ tels que $P((\mathfrak{M}, a_1, a_2, \ldots, a_n, c), (\mathfrak{N}', b_1, b_2, \ldots, b_n, d))$; par hypothèse d'induction, on a :

$$\mathfrak{N}' \models F[c, b_1, b_2, \ldots, b_n],$$

et donc $\mathfrak{N}' \models G[b_1, b_2, \ldots, b_n]$.

Comme $\mathfrak{N}'$ est une extension élémentaire de $\mathfrak{N}$, on a aussi :

$$\mathfrak{N} \models G[b_1, b_2, \ldots, b_n].$$

6°) Soient $\mathfrak{M}$ et $\mathfrak{N}$ deux modèles de A. En appliquant la résultat ci-dessus à ces deux modèles et à la suite vide, on voit que $\mathfrak{M}$ et $\mathfrak{N}$ satisfont les mêmes formules closes : deux modèles quelconques de A sont donc élémentairement équivalents et T est complète.

12 On va utiliser le lemme 2 de 1.3. Ajoutons n symboles de constante $c_0, c_1, \ldots, c_n$ au langage L et considérons la théorie :

$$\Phi = \{ H[c_0, c_1, \ldots, c_n] \text{ ; } H[v_0, v_1, \ldots, v_n] \text{ est une formule sans quantificateur de L et } T \vdash F[c_0, c_1, \ldots, c_n] \Rightarrow H[c_0, c_1, \ldots, c_n] \}.$$

Soit $\mathfrak{M}$ un modèle de $\Phi \cup T$. Considérons la théorie :

$$\Psi = \{K[c_0,c_1,...,c_n] \; ; \; K[v_0,v_1,...,v_n] \text{ est une formule sans quantificateur de L et } \mathfrak{M} \models K[c_0,c_1,...,c_n]\}.$$

On montre que $\Psi \cup T \cup \{F[c_0,c_1,...,c_n]\}$ est consistant : sinon, il existe un sous-ensemble fini Ψ_0 de Ψ tel que $\Psi_0 \cup T \cup \{F[c_0,c_1,...,c_n]\}$ est contradictoire. Il existe une formule sans quantificateur de L, $J[v_0,v_1,...,v_n]$, telle que :

$$J[c_0,c_1,...,c_n] = \bigwedge_{K \in \Psi_0} K, \quad \text{et} \quad T \vdash F[c_0,c_1,...,c_n] \Longrightarrow \neg J[c_0,c_1,...,c_n].$$

Il en découle que $\neg J[c_0,c_1,...,c_n]$ appartient à Φ, ce qui est absurde puisque $\mathfrak{M}$ est un modèle de Φ et satisfait $J[c_0,c_1,...,c_n]$.

Il existe un modèle $\mathfrak{N}$ de $\Psi \cup T \cup \{F[c_0,c_1,...,c_n]\}$. Les interprétaion de c_0, c_1,..., c_n dans $\mathfrak{M}$ et $\mathfrak{N}$ respectivement satisfont les mêmes formules atomiques : d'après le lemme 2 de 1.3, ils satisfont les mêmes formules, et $\mathfrak{M} \models F[c_0,c_1,...,c_n]$. On a donc montré que tout modèle de $\Phi \cup T$ satisfait $F[c_0,c_1,...,c_n]$.

On se sert encore du théorème de compacité : il existe un sous-ensemble fini Φ_0 de Φ tel que $F[c_0,c_1,...,c_n]$ soit conséquence de $\Phi_0 \cup T$. Soit $H[v_0,v_1,...,v_n]$ un formule sans quantificateur de L telle que

$$H[c_0,c_1,...,c_n] = \bigwedge_{K \in \Phi_0} K.$$

Alors $T \vdash F[c_0,c_1,...,c_n] \Longleftrightarrow H[c_0,c_1,...,c_n]$, et donc

$$T \vdash \forall v_0 \forall v_1 \quad \forall v_n (F[v_0,v_1,...,v_n] \Longleftrightarrow H[v_0,v_1,...,v_n]).$$

REMARQUE : Lorsque toute formule est équivalente, modulo T, à une formule sans quantificateur, on dit que T **admet l'élimination des quantificateurs**. Le raisonnement que l'on vient de présenter s'applique dans une situation beaucoup plus générale. Il montre en fait le théorème suivant : supposons que, pour tous modèles $\mathfrak{M}$ et $\mathfrak{N}$ de T et pour toutes suites $(a_0,a_1,...,a_n)$ et $(b_0,b_1,...,b_n)$ de M et N respectivement, si $(a_0,a_1,...,a_n)$ et $(b_0,b_1,...,b_n)$ satisfont les mêmes formules atomiques dans $\mathfrak{M}$ et $\mathfrak{N}$ respectivement, alors elles satisfont les mêmes formules. Alors T admet l'élimination des quantificateurs.

Par exemple, la théorie considérée à l'exercice 11 admet l'élimination des quantificateurs (grâce à la propriété démontrée en e),6°) de cet exercice).

13. Soit T une théorie exprimée dans un langage L qui est équivalente à une théorie finie. La thèorie T est donc équivalente à une seule formule close de L, que nous appellerons F. La classe des L-structures qui ne sont pas modèles de T est exactement la classe des L-structures qui sont modèles de $\neg F$, et par le théorème de Łos (théorème 4.3), cette classe est close par ultraproduit.

Réciproquement, supposons que T ne soit pas équivalente à une théorie finie. Pour chaque sous-ensemble fini X de T, il existe donc une L-structure $\mathfrak{M}_X$ qui est modèle de X mais pas de T. Appelons P l'ensemble des sous-ensembles finis de T et, pour chaque X de P, posons :

$$O(X) = \{Y \in P \; ; \; X \subseteq Y\}.$$

Si X_1, X_2, ..., X_n, sont des éléments de P, alors $O(X_1) \cap O(X_2) \cap \ldots \cap O(X_n)$ contient $X_1 \cup X_2 \cup \ldots \cup X_n$ et n'est donc pas vide. D'après le théorème 5.13 du chapitre 2, il existe un ultrafiltre $\mathcal{U}$ contenant l'ensemble $\{O(X) ; X \in P\}$. On va démontrer que :

$$\mathfrak{M} = \prod_{X \in P} \mathfrak{M}_X / \mathcal{U}$$

est un modèle de T. En effet, soit F une formule de T. Alors : $O(\{F\}) \in \mathcal{U}$, $O(\{F\}) \subseteq \{X \in P ; \mathfrak{M}_X \models F\}$, et donc $\{X \in P ; \mathfrak{M}_X \models F\} \in \mathcal{U}$. Ceci montre bien, avec le théorème de Łos, que $\mathfrak{M}$ satisfait F. On a donc trouvé des structures qui ne sont pas modèles de T et dont un ultraproduit est un modèle de T.

14. a) On a remarqué que la théorie des anneaux peut s'axiomatiser par des formules de Horn : donc un produit réduit de corps est un anneau. S'il s'agit d'un ultraproduit, par le théorème de Łos, c'est un corps.

Soient $\mathcal{F}$ un filtre sur un ensemble I, et, pour chaque $i \in I$, K_i un corps. Posons :

$$A = \prod_{i \in I} K_i / \mathcal{F}.$$

Suppsosons que $\mathcal{F}$ ne soit pas un ultrafiltre. Il existe donc un sous-ensemble I_0 de I tel que, ni I_0 lui-même, ni son complémentaire dans I n'appartiennent à $\mathcal{F}$. Pour chaque élément i de I, appelons respectivement $\mathbf{0}_i$ et $\mathbf{1}_i$ les éléments neutres de l'addition et de la multiplication dans le corps K_i. Considérons les fonctions a_0 et a_1 de I dans $\prod_{i \in I} K_i$ définis de la façon suivante :

- si $i \in I_0$, alors $a_0(i) = \mathbf{0}_i$ et $a_1(i) = \mathbf{1}_i$;
- si $i \notin I_0$, alors $a_0(i) = \mathbf{1}_i$ et $a_1(i) = \mathbf{0}_i$.

Soient $\bar{a}_0$ et $\bar{a}_1$ les éléments correspondants dans A. Alors, puisque

$$\{i \in I ; K_i \models a_0(i) = \mathbf{0}_i\} = I_0 \notin \mathcal{F}$$

par définition de produit réduit, $A \not\models \bar{a}_0 \simeq \mathbf{0}$; de même, $A \not\models \bar{a}_1 \simeq \mathbf{0}$. En revanche

$$\{i \in I ; K_i \models a_0(i) \times a_1(i) = \mathbf{0}_i\} = I,$$

et donc $A \models \bar{a}_0 \times \bar{a}_1 = \mathbf{0}$: l'anneau A n'est pas intègre, ce n'est pas un corps.

b) Découle immédiatement des définitions.

15. a) Voir l'exercice 18 du chapitre 3.

b) Par le théorème de Loweinheim-Skolem, on sait qu'il existe un sous-ensemble dénombrable X_0 de $\aleph_1$ tel que $\langle X_0, \leqslant \rangle \prec \langle \aleph_1, \leqslant \rangle$. Posons $\alpha_0 = \sup X_0$. On peut alors trouver un sous-ensemble X_1 dénombrable de $\aleph_1$ tel que $\alpha_0 \subseteq X_1$, et

$$\langle X_0, \leqslant \rangle \prec \langle X_1, \leqslant \rangle \prec \langle \aleph_1, \leqslant \rangle.$$

On continue et on définit par récurrence une suite de sous-ensembles dénombrables $(X_n ; n \in \mathbb{N})$ de $\aleph_1$ telle que, si $\alpha_n = \sup X_n$,

$$\alpha_n \subseteq X_n \quad \text{et} \quad \langle X_n, \leqslant \rangle \prec \langle X_{n+1}, \leqslant \rangle \prec \langle \aleph_1, \leqslant \rangle.$$

Posons $\alpha = \sup \{\alpha_n ; n \in \mathbb{N}\} = \bigcup_{n \in \mathbb{N}} X_n$. Par le théorème de l'union de chaîne de Tarski, (théorème 2.9), $\langle \alpha, \leqslant \rangle \prec \langle \aleph_1, \leqslant \rangle$.

c) On refait la même construction qu'au b) en partant d'un ensemble X_0 contenant un ordinal dénombrable α qui est tel que $<\alpha,\leqslant> \prec <\aleph_1,\leqslant>$. On obtient un autre ordinal dénombrable β, strictement supérieur à α, tel que :

$$<\beta,\leqslant> \prec <\aleph_1,\leqslant>.$$

Il en découle que $<\alpha,\leqslant> \prec <\beta,\leqslant>$.

En fait, cet argument (et le théorème de l'union de chaîne) montre que l'ensemble des ordinaux α tels que $<\alpha,\leqslant> \prec <\aleph_1,\leqslant>$ est un sous-ensemble clos cofinal de $\aleph_1$ (voir 20 au chapitre 7).

16. a) Comme chaque point de $\mathfrak{N}$ est l'interprétation d'un symbole de constante, T est en fait le diagramme complet de $\mathfrak{N}$. Il découle de 2.3 que tout modèle de T est isomorphe à une extension élémentaire de $\mathfrak{N}$.

b) Supposons que A et B soient deux sous-ensembles de $\mathbb{N}$, que $A \subseteq B$ et que $A \in \mathcal{F}_a$. Alors :

$$\mathfrak{N} \models \forall v_0(\underline{A}v_0 \Rightarrow \underline{B}v_0),$$

et donc, $\mathfrak{M} \models \forall v_0(\underline{A}v_0 \Rightarrow \underline{B}v_0)$.

et puisque $\mathfrak{M} \models \underline{A}a$, on en déduit $\mathfrak{M} \models \underline{B}a$, et $B \in \mathcal{F}_a$.

Supposons maintenant que A et B appartiennent tous les deux à $\mathcal{F}$. Posons $C = A \cap B$. Alors :

$$\mathfrak{N} \models \forall v_0((Av_0 \land Bv_0) \Rightarrow Cv_0),$$

d'où $\mathfrak{M} \models \forall v_0((Av_0 \land Bv_0) \Rightarrow Cv_0)$,

et, puisque $\mathfrak{M} \models \underline{A}a \land \underline{B}a$, on voit que $\mathfrak{M} \models \underline{C}a$, et $C \in \mathcal{F}_a$. Par ailleurs, la formule $\forall v_0 v_0 \notin \underline{\emptyset}$ est vraie dans $\mathfrak{N}$, donc dans $\mathfrak{M}$, et il en découle que $\emptyset \notin \mathcal{F}_a$.

Ceci montre donc que $\mathcal{F}_a$ est un filtre. Pour montrer que c'est un ultrafiltre, on se donne un sous-ensemble A de $\mathbb{N}$ et on appelle B son complémentaire. Alors

$$\mathfrak{N} \models \forall v_0(\underline{A}v_0 \lor \underline{B}v_0),$$

et donc $\mathfrak{M} \models \underline{A}a \land \underline{B}a$, ce qui montre soit A, soit B appartient à $\mathcal{F}_a$.

L'ultrafiltre $\mathcal{F}_a$ n'est pas trivial : si A est réduit à un seul élément n de $\mathbb{N}$, alors $\mathfrak{N} \models \forall v_0(\underline{A}v_0 \Rightarrow v_0 \simeq \underline{n})$. Comme $\mathfrak{M} \not\models a \simeq \underline{n}$, on voit que $A \notin \mathcal{F}$.

c) Si, pour une infinité d'entiers n, $f_r(n) = f_s(n)$, alors pour une infinité d'entiers n, $p_r(n)/q_r(n) = p_s(n)/q_s(n)$: les suites $(p_r(n)/q_r(n)\ ;\ n \in \mathbb{N})$ et $(p_s(n)/q_s(n)\ ;\ n \in \mathbb{N})$ ont donc même limite et $r = s$.

d) Soit $\mathfrak{M}$ un modèle de T non isomorphe à $\mathfrak{N}$. On veut montrer que la cardinalité de M est au moins $2^{\aleph_0}$. D'après ce qui a été dit au a) on peut supposer que $\mathfrak{M}$ est une extension élémentaire de $\mathfrak{N}$. Soit a un point de $\mathfrak{M}$ n'appartenant pas à $\mathbb{N}$. On va prouver que si r et s sont deux réels positifs distincts, alors :

$$\mathfrak{M} \models \neg \underline{f}_r a \simeq \underline{f}_s a,$$

ce qui montrera que l'application de $\mathbb{R}^+$ dans M qui à r fait correspondre l'interprétation de $\underline{f}_r(a)$ est injective, et donc que la cardinalité de M est au moins $2^{\aleph_0}$. Soit C l'ensemble

des entiers n tels que $f_r(n) = f_s(n)$. On vient de voir que C est fini, et donc, d'après b), $C \notin \mathcal{F}_a$ (parce qu'un ultrafiltre non trivial ne contient pas d'ensemble fini) et $\mathfrak{M} \models \neg\underline{C}a$. D'autre part, $\mathfrak{N} \models \forall v_0(f_r v_0 \simeq \underline{f}_s v_0 \Longleftrightarrow \underline{C}v_0)$ et donc,

$$\mathfrak{M} \models \forall v_0(\underline{f}_r v_0 \simeq \underline{f}_s v_0 \Longleftrightarrow \underline{C}v_0),$$

ce qui montre bien que $\mathfrak{M} \models \neg\underline{f}_r a \simeq \underline{f}_s a$.

Tous les modèles dénombrables de T sont donc isomorphes à $\mathfrak{N}$, donc T est $\aleph_0$-catégorique.

e) Le modèle $\mathfrak{N}$ n'a qu'un seul enrichissement $\mathfrak{N}'$ en une L'-structure qui soit un modèle de T' : celui où le symbole X est interprété par l'ensemble $\mathbb{N}$ tout entier. Tout modèle dénombrable de T' est alors isomorphe à $\mathfrak{N}'$ (son L-réduit étant isomorphe à $\mathfrak{N}$).

Pourtant T', qui n'admet évidemment pas de modèles finis, n'est pas complète : la formule $\forall v_0 X v_0$ est vraie dans $\mathfrak{N}'$, mais on peut trouver un modèle de T' dans lequel elle n'est pas vérifiée : on choisit une extension élémentaire propre de $\mathfrak{N}$ et on interprète X par l'ensemble $\mathbb{N}$.

Cet exemple montre que, dans le théorème de Vaught (2.6), on ne peut pas se passer de l'hypothèse : « κ supérieur ou égal à card(L) ».

17. a) C'est une conséquence immédiate du théorème 2 de 5.1 au chapitre 3.

b) On raisonne par l'absurde. Soit F une formule de T et $\mathfrak{M}$ un modèle de $T \cup U(\neg F)$. D'après l'exercice 19 (b) du chapitre 3, il existe un modèle $\mathfrak{M}'$ de $\neg F$ tel que $\mathfrak{M}$ se plonge dans $\mathfrak{M}'$. Or $\mathfrak{M}$ est un modèle de T et T est préservée par extension. Donc $\mathfrak{M}'$ est aussi un modèle de T ; mais $\mathfrak{M}'$ est un modèle de $\neg F$ et $F \in T$: contradiction.

c) Soit F une formule de T. Puisque $T \cup U(\neg F)$ est contradictoire, on peut trouver (compacité) des formules $H_1, H_2, \ldots, H_k$, en nombre fini, dans $U(\neg F)$, telles que $T \cup \{H_1, H_2, \ldots, H_k\}$ soit contradictoire, ce qui revient à dire que la formule $\neg(H_1 \wedge H_2 \wedge \ldots \wedge H_k)$ est conséquence de T. La formule $(H_1 \wedge H_2 \wedge \ldots \wedge H_k)$, conjonction de formules universelles conséquences de $\neg F$, est équivalente à une formule universelle, disons G_F, qui sera aussi conséquence de $\neg F$. On a bien $T \vdash \neg G_F$.

d) Posons $T' = \{\neg G_F ; F \in T\}$. On vient de le voir, chaque formule de T' est conséquence de T. Réciproquement, pour chaque formule $F \in T$, G_F est conséquence de $\neg F$, ce qui équivaut à dire que F est conséquence de $\neg G_F$; a fortiori, F est conséquence de T'. Les théories T et T' sont donc équivalentes. Comme chacune des G_F est universelle, chaque formule de T' est équivalente à une formule existentielle. Ainsi T est équivalente à une théorie existentielle.

BIBLIOGRAPHIE

Nous proposons tout d'abord une liste (certainement très incomplète) d'ouvrages traitant de logique mathématique. Il s'agit soit de traités généraux sur la logique, soit de livres plus spécialisés sur certains des sujets que nous avons abordés. Une exception, toutefois : le livre édité sous la direction de J. Barwise, dont l'ambition était de faire le point, à l'époque où il a été publié, des connaissances en logique.

J.P. Azra et **B. Jaulin**, *Récursivité*, Gauthiers-Villars, 1973.

J. Barwise (sous la direction de), *Handbook of mathematical logic*, North-Holland, 1977.

J.L. Bell et **A.B. Machover**, *A course in mathematical logic*, North-Holland, 1977.

J.L. Bell et **A.B. Slomson**, *Models and ultraproducts*, North-Holland, 1971.

E.W. Beth, *Formal methods*, D. Reidel publishing company, 1962.

C.C. Chang et **J.H. Keisler**, *Model Theory*, North-Holland, 1973.

A. Church, *Introduction to mathematical logic*, Princeton University Press, 1956.

P. Cohen, *Set theory and the continuum hypothesis*, W.A. Benjamin, 1966.

H. Curry, *Foundation of mathematical logic*, McGraw-Hill, 1963.

D. van Dalen, *Logic and structures*, Springer-Verlag, 1983.

M. Davis, *Computability and unsolvability*, McGraw-Hill, 1958.

F. Drake, *Set theory*, North-Holland, 1979.

H.D. Ebbinghaus, **J. Flum** et **W. Thomas**, *Mathematical logic*, Springer-Verlag, 1984.

R. Fraïssé, *Cours de logique mathématique*, Gauthier-Villars, 1972.

J.Y. Girard, *Proof theory*, Bibliopolis (Naples), 1987.

P. Halmos, *Lectures on Boolean algebras*, D. Van Nostrand, 1963.

P. Halmos, *Naive set theory*, D. Van Nostrand, 1960. Traduction française parue chez Gauthier-Villars.

D. Hilbert et **W. Ackermann**, *Mathematical logic*, Chelsea publishing company, 1950.

K. Hrbacek et **T. Jech**, *Introduction to set theory*, Marcel Dekker (New York, Basel), 1984.

T. Jech, *Set theory*, Academic Press, 1978.

S. Kleene, *Logique mathématique* (traduit de l'anglais), Armand Colin, 1971 ; réédité chez J. Gabay en 1987.

G. Kreisel et **J.L. Krivine**, *Eléments de logique mathématique*, Dunod, 1966.

J.L. Krivine, *Théorie axiomatique des ensembles*, PUF, 1969.

K. Kunen, *Set theory*, North-Holland, 1985.

R. Lalement, *Logique, réduction, résolution*, Masson 1990.

R.C. Lyndon, *Notes on logic* D. Van Nostrand, 1966.

A.I. Mal'cev, *The metamathematics of algebraic systems*, North-Holland, 1971

Y. Manin, *A course in mathematical logic* (traduit du russe), Springer-Verlag, 1977.

J. Malitz, *An introduction to mathematical logic*, Springer-Verlag, 1979.

M. Margenstern, *Langage Pascal et logique du premier ordre*, Masson, 1989 et 1990.

E. Mendelson, *Introduction to mathematical logic*, D. Van Nostrand, 1964.

P.S. Novikov, *Introduction à la logique mathématique* (traduit du russe), Dunod, 1964.

P. Odifreddi, *Classical recursion theory*, North Holland, 1989.

J.F. Pabion, *Logique mathématique*, Hermann, 1976.

R. Péter, *Recursive functions*, Academic Press, 1967.

B. Poizat, *Cours de théorie des modèles*, Nur al-Mantiq wal-Ma'rifah (diffusé par Offilib, Paris), 1985.

D. Ponasse, *Logique mathématique*, O.C.D.L., 1967.

W. Quine, *Mathematical logic*, Harvard University Press, 1951.

W. Quine, *Méthodes de logique*, Rinehart and Winston, 1950 et 1972. Traduction française parue chez Armand Colin, 1973.

H. Rasiowa et **R. Sikorski**, *The mathematics of metamathematics*, PWN-Polish Scientific Publishers, 1963.

A. Robinson, *Complete theories*, North-Holland, 1956.

A. Robinson, *Introduction to model theory and to the metamathematics of algebra*, North-Holland, 1974.

H. Rogers, *Theory of recursive functions and effective computability*, McGraw-Hill, 1967.

J.B. Rosser, *Logic for mathematicians*, McGraw-Hill, 1953.

J.R. Shoenfield, *Mathematical logic*, Addison-Wesley, 1967.

W. Sierpinski, *Cardinal and ordinal numbers*, PWN-Polish Scientific Publishers, 1965.

R. Sikorski, *Boolean algebras*, Springer-Verlag, 1960.

R. Smullyan, *First order logic*, Springer-Verlag, 1968.

R.I. Soare, *Recursively enumerable sets and degrees*, Springer-Verlag, 1987.

J. Stern, *Fondements mathématiques de l'informatique*, McGraw-Hill, 1990.

P. Suppes, *Axiomatic set theory*, D. Van Nostrand, 1960.

P. Suppes, *Introduction to logic*, D. Van Nostrand, 1957.

K. Shütte, *Proof theory*, Springer-Verlag, 1977.

A. Tarski, *Introduction to logic and to the methodology of deductive sciences*, Oxford University Press, 1965.

A. Tarski, A. Mostowski, R. Robinson, *Undecidable theories*, North-Holland, 1953.

R.L. Vaught, *Set theory, Birkhaüser*, 1985.

Pour compléter cette bibliographie, le lecteur curieux ou éclectique trouvera ci-dessous des références de livres ayant un intérêt historique et d'ouvrages à caractère récréatif, tous en rapport avec notre propos.

L. Carroll, *Logique sans peine* (traduit de l'anglais), Hermann, 1972.

M. Gardner, *La magie des paradoxes*, Bibliothèque POUR LA SCIENCE (diffusion Belin), 1980.

K. Gödel, *Collected works*, publié sous la direction de S. Feferman, Oxford University Press, 1986.

J. van Heijenoort, *From Frege to Gödel, a source book in mathematical logic (1879-1931)*, Harvard University Press, 1967.

A. Hodges, *Alan Turing ou l'énigme de l'intelligence* (traduit de l'anglais), Bibliothèque scientifique Payot, 1988.

R. Smullyan, *Le livre qui rend fou* (traduit de l'anglais), Bordas-Dunod, 1984.

J. Venn, *Symbolic logic*, Chelsea publishing company, 1971 (première édition : 1881).

NOTATIONS

Tome I

Mode d'emploi

Chapitre 1

Chapitre 2

Chapitre 3

Chapitre 4

Tome II

Mode d'emploi

Chapitre 5

Chapitre 6

Chapitre 7

Chapitre 8

Solutions des exercices du tome II

INDEX

Le numéro en chiffres romains indique le tome ; par exemple, II.319 renvoie à la page 319 du deuxième tome.

045453 - (I) - (1) - OSB 80° - RET - CDD

Achevé d'imprimer sur les presses de la
SNEL S.A.
Rue Saint-Vincent 12 – B-4020 Liège
tél. 32(0)4 344 65 60 - fax 32(0)4 343 77 50
janvier 2003 – 27127

Dépôt légal : janvier 2003
Imprimé en Belgique

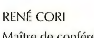
SCIENCES SUP



René Cori
Daniel Lascar

LOGIQUE MATHÉMATIQUE

2. Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles



Domaine d'une grande richesse, la logique mathématique donne lieu à des découvertes théoriques majeures. L'explosion de l'informatique, avec des applications et des intuitions nouvelles, lui a fourni une impulsion décisive et inédite.

Ce cours, enseigné à l'université, traite de manière détaillée des domaines fondamentaux de la logique mathématique. Dans le premier tome sont exposés le calcul propositionnel, les algèbres de Boole, le calcul des prédicats et les théorèmes de complétude. Ce second tome est consacré aux problèmes de récursivité et de formalisation de l'arithmétique, aux théorèmes de Gödel et à la théorie des ensembles ainsi qu'à la théorie des modèles. Outre le cours, de nombreux exercices corrigés permettront au lecteur d'acquérir et de maîtriser les différentes notions exposées.

L'ouvrage se destine principalement aux étudiants en licence, master et doctorat de logique, mathématique et informatique. Il intéressera également les élèves ingénieurs et les étudiants désirant s'orienter vers les mathématiques pures ou l'informatique, ainsi que les chercheurs et les ingénieurs de recherche en informatique.

RENÉ CORI
Maître de conférences à l'université Denis-Diderot, Paris 7.

DANIEL LASCAR
Directeur de recherches au CNRS.

MATHÉMATIQUES
PHYSIQUE
CHIMIE
SCIENCES DE L'INGÉNIEUR
INFORMATIQUE
SCIENCES DE LA VIE
SCIENCES DE LA TERRE





ISBN 2 10 005453 8

http://www.dunod.com